BULLETIN OF NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
ISSN 1991-3494
Volume 2, Number 354 (2015), 208 – 211

WAYS OF ENSURING INFORMATION SECURITY

A. D. Kazbayeva, G. B. Kashaganova

Kazakh National Technical University named after K. I. Satpayev, Almaty, Kazakhstan.
E-mail: alua6@mail.ru, guljan_k70@mail.ru

Keywords: computer network, information security, corporate information systems.

Abstract. This article discusses problems and ways of safety of computer systems and networks, measures legislative, administrative and organizational, program technological level; solutions of problems of information security in networks.

ӘОЖ 378: 004

АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ ТӘСІЛДЕРІ

А. Д. Қазбаева, Г. Б. Қашағанова

Қ. И. Сәтбаев атындағы Қазақ ұлттық техникалық университеті, Алматы, Қазақстан

Тірек сөздер: компьютерлік желі, ақпараттық қауіпсіздік, корпоративті ақпараттық жүйе.

Аннотация. Мақалада компьютерлік жүйелер мен желілердің қауіпсіздігін қамтамасыз ету мәселелері, қауіпсіздікті қамтамасыз ету мәселесін шешуге арналған тәсілдер жайлы айтылады.

Компьютерлік жүйелер мен желілердің (КЖ) қауіпсіздігін қамтамасыз ету мәселесінің екі тәсілі бар: «көріністік» және кешендік.

«Фрагменттік» тәсіл шартта көрсетілген нақты анықталған қауіптерге қарсы бағытталған. Мұндай тәсілдерді жүзеге асырудың мысалы ретінде шифрлеудің автономдық құралдарын, арнайы антивирустік бағдарламалар және т.б. жеке рұқсат беру басқару құралдарын айтуға болады.

Мұндай тәсілдің жетістігі нақты қауіпке жоғары талдау жасау болып табылады. Маңызды кемшілігі – ақпаратты өңдеудің бірыңғай қауіпсіз ортасының болмауы. Ақпаратты қорғаудың фрагменттік тәсілдері компьютерлік жүйелер мен желілердің нақты объектілерін нақты қауіп-терден қорғауды қамтамасыз етеді. Тіпті, қауіп түрінің азғантай өзгеруі қорғау тиімділігінің жоғалып кетуіне әкеп соғады.

Кешендік тәсіл қауіпке қарсы тұрудың әртүрлі тәсілдерін бірыңғай кешендерге біріктіретін, КЖ ақпаратты өңдеудің қауіпсіздік ортасын құруға бағытталған. Ақпаратты өңдеудің қауіпсіздік ортасын ұйымдастыру – кешендік тәсілдің сөзсіз жетістігі болып табылады, КЖ қауіпсіздігінің белгілі деңгейін сақтауға мүмкіндік береді. Бұл тәсілдің кемшіліктері: КЖ пайдаланушылардың еркін әрекет етуіне шектеу қою, қауіпсіздік құрылғыларын орнату және жөндеу кезіндегі қателерге сезімталдығы, басқару қиыншылығы.

Кешендік тәсіл жауапты тапсырмаларды орындаушы немесе ерекше маңызды ақпараттарды өңдейтін шағын КЖ мен ірі ұйымдардың КЖ қорғау үшін қолданады. Ірі ұйымдардың КЖ ақпарат қауіпсіздігінің бұзылуы ұйымдардың өздеріне, сондай-ақ, олардың клиенттеріне де орасан зор материалдық нұқсан келтіруі мүмкін. Сондықтан, мұндай ұйымдар қауіпсіздікті сақтауға ерекше

назар аударуға және кешендік қорғауды жүзеге асыруға мәжбүрлі. Кешендік тәсіл көптеген мемлекеттік және ірі коммерциялық кәсіпорындар мен мекемелерді ұстап тұр. Бұл тәсіл әртүрлі стандарттарда өзінің орнын тапқан.

Қауіпсіздікті қамтамасыз ету мәселесіне арналған кешендік тәсіл нақты КЖ үшін құрылған қауіпсіздік саясатқа негізделген. Қауіпсіздік саясаты КЖ қорғау құралының тиімді жұмысын регламенттейді. Ол жүйенің әртүрлі жағдайдағы әрекеттерін анықтай отырып, ақпаратты өңдеу құбылысының барлық ерекшеліктерін қамтиды. Желілердің сенімді қауіпсіздік жүйесі желілік қауіпсіздіктің тиімді саясатынсыз құрылуы мүмкін емес [1].

Ақпараттық қарым-қатынас субъектілерінің қызығушылығын қорғау үшін келесі деңгейлердің шараларын байланыстыру қажет:

– заңнамалық (стандарттар, заңдар, нормативтік актілер және т.б.);

– административтік-ұйымдастырушылық (ұйымдар басшылығымен қабылданған және адамдармен байланысы бар қауіпсіздіктің нақты шаралары, жалпы сипаттың әрекеті);

– бағдарламалық-техникалық (нақты техникалық шаралар).

Заңнамалық деңгейлер шарасы ақпараттық қауіпсіздікті қамтамасыз ету үшін өте маңызды. Бұл деңгейге ақпараттық қауіпсіздікті бұзушыға кері көзқарасты қоғамда құруға және қолдауға бағытталған шаралар кешені жатады.

Ақпараттық қауіпсіздік – ол қызметтің жаңа саласы, мұнда тек тыйым салу мен шара қолдану ғана емес, үйрету, түсіндіру, көмектесу де маңызды. Қоғам бұл мәселелердің маңыздылығын жете түсінуі керек, осыған сәйкес мәселелердің негізгі жолдарын түсінуі қажет. Мемлекет мұны тиімді етіп жасауына болады. Мұнда үлкен материалдық шығынның қажеті жоқ, интеллектуалдық қаржы жұмсау қажет.

Административтік-ұйымдастырушылық деңгейдің шаралары. Ұйымдардың администраторлары қауіпсіздік тәртіптерін қолдаудың қажеттілігін ұғынуы қажет және осы мақсаттарға сай қор бөлуі қажет. Административтік-ұйымдастырушылық деңгейдің негізгі қауіпсіздік шаралары болып, қауіпсіздік саясаты және ұйымдастыру шараларының кешені болып табылады.

Ұйымдастыру шараларының кешеніне адамдардың жүзеге асырған қауіпсіздік шаралары жатады.

Ұйымдастыру шараларын келесі топтарға бөледі:

– қызметкерлерді басқару;

– физикалық қорғау;

– жұмыс қабілеттілігін қолдау;

– қауіпсіздік тәртібінің бұзылуын сезіну;

– қайта орнына келтірілген жұмысты жобалау.

Әрбір ұйымдарда, әрбір топтар үшін қызметкерлердің іс-әрекетін анықтайтын регламенттер жиынтығы болуы қажет [2].

Бағдарламалық-техникалық деңгейдің шаралары мен құралдары. Акпараттық қауіпсіздік тәртібін қолдау үшін ақпараттық-техникалық деңгейдің шаралары маңызды, өйткені, компьютерлік жүйенің негізгі қаупі олардың өздерінен басталады, әсіресе, құрылғылардың жұмыс істемей қалуы, бағдарламалық қамтамалардың қателесуі, пайдаланушылар мен администраторлардың ағаттықтары және т.б. Заманауи ақпараттық жүйелер шеңберінде келесі қауіпсіздік механизмдері қол жетімді болуы қажет:

– идентификация және пайдаланушының дұрыстығын тексеру;

– қол жетімділікті басқару;

– хаттамалау және аудит;

– криптография;

– firewall;

– жоғары қол жетімділікті қамтамасыз ету.

Стандарттарды қолдану қажеттілігі. Компанияның ақпараттық жүйелері (АЖ) әрқашан да әртүрлі өндірушінің бағдарламалық және аппараттық өнімдерінің негізінде құрылған. Қазіргі кезде заманауи АЖ құру үшін пайдаланушыға құралдардың толық тізімін (аппараттықтан бастап бағдарламалыққа дейін) ұсынатын бірде-бір жасаушы компания жоқ. Ақпаратты сенімді қорғаудың әркелкі АЖ қамтамасыз ету үшін АЖ әрбір компонентінің қауіпсіздігіне жауапты жоғары білікті

маман талап етіледі: оларды дұрыс жөндеу, болған өзгертулерді ылғи қадағалап отыру, пайдаланушылардың жұмысын бақылау. АЖ әртүрлі болғандықтан, оның қауіпсіздігін қамтамасыз ету де күрделірек. Корпоративті желілер мен қауіпсіздік жүйе құрылғыларында желіаралық қалқандардың (firewall), шлюздер мен VPN көптігі, сондай-ақ қызметкерлер, серіктестер және тапсырыс берушілер жағынан корпоративті желі мәліметтерге қол жетімділіктің үдемелі сұранысы басқаруға қиын, ал кейде үйлеспейтін күрделі қауіпсіздік ортасын құруға әкеп соғады.

Қорғау өнімдерінің интероперабельділігі КАЖ үшін айырып алғысыз талап болып табылады. Көптеген гетерогендік орталар үшін басқа пайдаланушылардың өнімдерімен келісілген өзара әрекетті қамтамасыз ету маңызды. Ұйымдар қабылдаған қауіпсіздік шешімі осы ұйым шеңберінде барлық платформадағы қауіпсіздікке кепіл беру қажет. Сондықтан да қауіпсіздік құрылғыларымен қамтамасыз етушілердің, сонымен қатар компаниялардың (өздерінің корпоративті жүйелер мен желілеріне қауіпсіздік жүйесіне тапсырыс беруші ретінде шығады) – жүйелік интеграторлар мен ұйымдардың бірыңғай стандарттар жиынын қолдану қажеттілігі толықтай айқын. Стандарттар ақпараттық қауіпсіздікті қамтамасыз етуде барлық жұмыс жасалатын түсінікті базисті құрады. Стандарттар гетерогендік ортада желі қауіпсіздік жүйесін құру кезінде өте маңызды, түрлі өндірушілердің өнімдерінің бірлесуін қамтамасыз ететін қажетті негіз болып табылады.

Қауіпсіздікті қамтамасыз ету мәселесін шешуге арналған кешенді тәсіл, заңнамалық, административтік-ұйымдастырушылық және бағдарламалық-техникалық шаралардың тиімді байланысын шешу және өнеркәсіптік, ұлттық және халықаралық стандарттарды міндетті қадағалау – осылар барлық корпоративтік желілер жүйесін құратын фундамент болып табылады [3].

Желіде ақпаратты қорғау мәселелерін шешу жолдары.

Интернет желісінде жұмыс жасағанда ақпараттық қауіпсіздік мәселесінің шешімін табу үшін ISTF (Internet Security Task Force) тәуелсіз бірлестігі құрылды. ISTF (Internet Security Task Force) – ақпараттық қауіпсіздік құралдарымен қамтамасыз етуші компания эксперттері мен өкілдерінен, Internet-инфрақұрылымы провайдері мен электронды бизнестерден тұратын қоғамдық ұйым. Консорциумның мақсаты – Internet-пен жұмыс кезінде қауіпсіздік бойынша техникалық, ұйымдық және операциялық нұсқаулықтар құру.

ISTF консорциумі ақпараттық қауіпсіздіктің 12 облысын белгіледі, оның жұмыс қабілеттілігін қамту үшін, оған ең бірінші электронды бизнесті құрушылардың назарын аударту керек. Бұл тізімге төмендегілер кіреді:

– аутентификация (идентификацияланған ақпартты растайтын механизмі);
– жеке және дербес ақпаратқа ие болу құқығы (ақпараттың құпия болуын қамтамасыз ету);
– қауіпсіздік оқиғаларын анықтау (Security Events);
– корпоративті периметр қауіпсіздігі;
– шабуылдарды анықтау;
– аса қауіпті әрекеттерді бақылау;
– әкімшілік басқару (администрирование);
– оқиғаға реакциясы (Incident Response). ISTF ұсыныстары ертеден келе жатқан және енді құрылған электронды бизнес және электронды сауда компанияларына арналған.

Олардың жүзеге асуы электронды бизнес жүйесіндегі ақпаратты қауіпсіздігі кешенді болу керек екенін білдіреді.

Қауіптерден кешенді қорғану үшін және электронды бизнес үшін экономикалық тиімді болуына кепіл беру және коммуникациялық ресурстарды қауіпсіз қолдану үшін:

– электронды бизнес жүйесі үшін қауіпсіздікке қатер төнетін әрекеттерді талдау;
– ақпараттық қауіпсіздік саясатын құру;
– мәліметтер жіберілетін сыртқы каналдарды қорғап, ақпараттың құпия болуын, тұтастығын, түпнұсқалылығын қамтамасыз ету;
– Internet және сыртқы желідегі ашық ресурстарға рұқсат алуының қауіпсіз болу мүмкіндігіне кепіл беру, сонымен қатар, желі ішіндегі қолданушылардың қарым-қатынасының қауіпсіз болуына кепіл беру;
– персоналға корпоративті желідегі ақпараттық ресурстарға қауіпсіз ұзақ арақашықтан қол жеткізуіне мүмкіндік беру;
– желі қауіпсіздік құралдарын сенімді орталықтандырып, басқаруын қатамасыз ету.

ISTF ұсыныстарына сәйкес электронды бизнесте ақпараттық қауіпсіздік жүйесін құрудың бірінші және маңызды этапы желідегі ортақ ресурстарды қолдануға қол жеткізуді басқару механизмі болып табылады, сонымен қатар, VPN виртуалды қауіпсіз желі өнімдерімен және брандмауэр арқылы жүзеге асатын қауіпсіз коммуникация механизмі. Оларды біріктіру қаражаты арқылы жөнелту және қауіпсіздік жүйесінің барлық маңызды ақпараттарын басқару арқылы ақпараттық қауіпсіздіктің орталықтан басқарылатын және біртұтас жүйесін алуға болады.

Корпоративті жүйенің барлық деңгейінде кешенді қауіпсіздік құралдарын қолдану тиімді және сенімді ақпараттық қауіпсіздік қамтамасы жүйесін құруға мүмкіндік береді.

ӘДЕБИЕТ

[1] Лукацкий А.В. Обнаружение атак. – СПб., 2001. – 624 с.
[2] Сбиба В.Ю, Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности.
[3] <http://www.wikipedia.org> – интернет-энциклопедия.

REFERENCES

[1] Lukatsky A.B. *Detection of attacks.* St. Petersburg, **2001.** – 624 p. (in Russ).
[2] Sbiba V.Yu., Kurbatov V.A. *Guide to protection from internal threats of information security.* (in Russ).
[3] <http://www.wikipedia.org> – internet encyclopedia. (in Russ).

СПОСОБЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А. Д. Казбаева, Г. Б. Кашаганова

Казахский национальный технический университет им. К. И. Сатпаева, Алматы, Казахстан

Ключевые слова: компьютерная сеть, информационная безопасность, корпоративные информационные системы.

Аннотация. В статье рассматриваются проблемы и способы обеспечения безопасности компьютерных систем и сетей; меры законодательного, административно-организационного, программно-технического уровня; пути решения проблем защиты информации в сетях.

Поступила 20.03.2015 г.