Дәріс 10. Аутентификация. Әлсіз парольдер. Unix-тегі құпия сөзді қорғау. Бір реттік парольдер

Жоспары:
1Аутентификация және оның талап етілуі
2Әлсіз парольдар
3Unix-тегі құпия сөзді қорғау
4Бір реттік парольдер

Әрбір сенімді (secured) компьютерлік жүйе кіру кезінде барлық пайдаланушылардан аутентификацияны талап етуі керек. Өйткені, егер операциялық жүйе пайдаланушының кім екеніне сенімді бола алмаса, ол қандай файлдарға және басқа ресурстарға қол жеткізе алатындығын біле алмайды. Аутентификация тақырыбы тым маңызды емес болып көрінуі мүмкін, бірақ бұл күткеннен әлдеқайда қиын. Пайдаланушының аутентификациясы "Онтогенез филогенезді қайталайды" және қарастырылған нәрселерге қатысты. ENIAC сияқты әмбебап машиналардың алғашқы модельдерінде жүйеге кіру процедурасын айтпағанда, Операциялық жүйе болған жоқ. Кейінгі пакеттік жүйелер мен уақытты бөлу жүйелері, әдетте, тапсырмалар мен пайдаланушыларды аутентификациялау үшін кіру процедураларына ие болды. Алғашқы шағын компьютерлерде (мысалы, PDP-1 және PDP-8) кіру процедурасы болған жоқ, бірақ UNIX операциялық жүйесінің PDP-11 шағын компьютеріне таралуымен бұл процедура қайтадан сұранысқа ие болды. Алғашқы дербес компьютерлерде (мысалы, Apple II және IBM PC бастапқы нұсқасы) кіру процедурасы болған жоқ, бірақ ол Linux және Windows 8 сияқты жеке компьютерлерге арналған күрделі операциялық жүйелерде пайда болды (бірақ қысқа мерзімді пайдаланушылар оны өшіре алады). Сонымен, қазіргі уақытта көптеген адамдар интернет-банкингті пайдалану, электронды сатып алу, музыка жүктеу және басқа да әрекеттерді орындау мақсатында қашықтағы компьютерлер жүйесіне кіреді (жанама түрде). Барлық осы әрекеттер аутентификацияланған кіруді қажет етеді. Аутентификацияның маңыздылығына көз жеткізгеннен кейін оны жүзеге асырудың қолайлы әдісін іздеуге көшу керек. Пайдаланушыларды кіруге тырысқанда аутентификацияның көптеген әдістері үш негізгі қағидаға негізделеді, атап айтқанда: пайдаланушыға белгілі бір нәрсеге сүйену; қолданушыда бар нәрсеге сүйену; ол білдіретін нәрсеге сүйену. Кейде олардың екеуі қосымша қауіпсіздік шараларын қажет етеді. Осы принциптердің негізінде өзіндік күрделілігі мен қауіпсіздік қасиеттері бар аутентификацияның әртүрлі схемалары жасалады. Олардың барлығы кезек бойынша келесі бөлімдерде қаралатын болады. Пайдаланушыдан тіркеу аты мен парольді енгізуді талап ететін аутентификация нысаны кеңінен қолданылды. Құпия сөзді қорғауды түсіну және жүзеге асыру оңайырақ. Ең қарапайым іске асыру жұптардың негізгі тізілімін (тіркеу аты, пароль) қолдау болып табылады. Енгізілген тіркеу атауы тізілімде ізделеді және енгізілген пароль сақталған

парольмен салыстырылады. Егер олар сәйкес келсе, кіруге рұқсат етіледі, егер жоқ болса, ол қабылданбайды. Монитордың жанында орналасқан қызықты көздерден жасыру үшін әрдайым енгізілетін құпия сөз экранда көрсетілмейді. Windows жүйесінде әр терілген таңба Жұлдызшамен көрсетіледі. Unix жүйесінде парольді енгізу кезінде ештеңе көрсетілмейді. Бұл екі схема әртүрлі қасиеттерге ие. Windows жүйесінде қолданылатын Схема ұмытылған пайдаланушыларға терілген таңбалардың санын бақылауды жеңілдетеді, бірақ сонымен бірге құпия сөздің ұзындығын ашады. Қауіпсіздік тұрғысынан үнсіздік-бұл алтын. Қателіктер қауіпсіздік деңгейіне айтарлықтай әсер етуі мүмкін, тағы бір сала 1-суретте көрсетілген. Жүйе хабарламаларды жоғарғы регистрде көрсетіп, пайдаланушы төменгі регистрде енгізген кезде сәтті кіру 1, а-суретте көрсетілген. 1, б-суретте крекердің а жүйесіне кіруге сәтсіз әрекеті көрсетілген, ал 1, в- суретте хакердің В жүйесіне кіру әрекеті сәтсіз аяқталды.

1-сурет. Жүйеге кіру: а-сәтті; б-атын енгізгеннен кейін кіруден бас тарту; в-аты мен паролінен енгізгеннен кейін кіруден бас тарту

1-суреттегі В жүйесі қате тіркеу атауын көргеннен кейін кіруден бас тартады. Бұл қате деп саналады, өйткені бұзушыға тиісті атау табылғанға дейін Тіркеу атауын таңдауды жалғастыруға мүмкіндік береді. 15-суретте бұзушыдан әрқашан пароль сұралады және ол енгізген тіркеу аты сәйкес келе ме, жоқ па, оған хабарланбайды. Ол тек тіркеу аты мен парольдің тіркесімі жарамсыз екенін біледі. Кіру процедураларынан басқа, көптеген Ноутбуктер жоғалған немесе ұрланған жағдайда олардың мазмұнын қорғау үшін тіркеу аты мен парольді қажет етеді. Әрине, бұл ештеңеден жақсы, бірақ көп емес. Кез-келген ноутбук қуатты қосып, BIOS орнату бағдарламасына Del немесе F8 пернесін немесе амалдық жүйені іске қоспас бұрын BIOS параметрлерін шақыруға байланысты басқа пернелерді (әдетте экранда көрсетілетін ақпарат) басып тұрып кіре алады. Орнату бағдарламасында ол қатты дискіні іске қоспас бұрын компьютерді USB флэш-дискісінен бастауға нұсқау беру арқылы қолданылатын іске қосу құрылғыларының тізбегін өзгерте алады. Содан кейін табылған ноутбук толық операциялық жүйесі бар USB флэш-дискісін салып, компьютерді осы дискіден іске қосады. Амалдық жүйені іске қосқаннан кейін қатты дискіні орнатуға болады (UNIX-те) немесе d: құрылғысы ретінде қол жетімді (Windows-та). Осындай жағдайдың алдын алу үшін көптеген BIOS жүйелері қолданушыға BIOS теңшеу бағдарламасын парольмен қорғауға мүмкіндік береді, осылайша тек пайдаланушы жүктеу кезінде құрылғылардың сауалнама тізбегін өзгерте алады. Егер сіз ноутбукты қолдансаңыз, кітап оқуды тоқтатып, BIOS-қа құпия сөзді орнатып, оқуға оралыңыз.

Әлсіз парольдер. Көбінесе бұзушылар жүйеге кіріп, жоспарланған компьютерге (мысалы, Интернет арқылы) қосылып, қолданыстағы комбинациялардың бірін тапқанша көптеген комбинацияларды (тіркеу аты, пароль) сұрыптайды. Көптеген адамдар қандай-да бір түрде тіркеу атауында өздерінің нақтыатын қолданады.

Мысалы, Ellen Ann Smith үшін ellen, smith, ellen smith, ellen-smith, ellen тиісті нұсқалары болуы мүмкін. smith, esmith, easmith және eas. "Сіздің жаңа туған нәрестеңізге арналған 4096 есім" сияқты кітаптардың бірімен және фамилиялармен толтырылған телефон кітабымен қаруланған крекер жүйеге шабуыл жасайтын ел үшін ықтимал тіркеу атауларының компьютерленген тізімін оңай жасай алады (ellen_smith АҚШ-та немесе Ұлыбританияда бірдей жұмыс істей алады,бірақ Жапонияда емес). Әрине, тек тіркеу атауын шешу жеткіліксіз. Әлі бәсекелік пароль. Мұны істеу қиын ба? Сіз ойлағаннан әлдеқайда оңай.

UNIX жүйелеріндегі парольдердің қауіпсіздігі бойынша классикалық жұмысты Моррис пен Томпсон жасаған (Моррис және Томпсон, 1979). Олар Ықтимал парольдердің тізімін жасады:атаулар мен фамилиялар, көше атаулары, қала атаулары, орташа сөздіктердегі сөздер (сонымен қатар кері жазудағы сөздер), тіркеу нөмірлері және т.б. содан кейін олар сәйкестіктерді іздеудегі жүйелік пароль файлымен салыстырды. Барлық парольдердің 86% - дан астамы олардың тізімінде табылды. Егер біреу жоғары білікті пайдаланушылар сәтті парольдерді таңдайды деп ойласа, мен сендіре аламын: олай емес. 2012 жылы 6,4 миллион LinkedIn құпия сөздері бұзылғаннан кейін Интернетке кірген кезде, көптеген нәтижелерді талдау қызықты болды. Ең танымал пароль "пароль" сөзі болды. Ең танымал екінші пароль "123456" болды (еңтанымал ондыққа "1234", "12345" және "12345678"кірді). Олардың тұрақтылығы туралы айтудың қажеті жоқ. Шын мәнінде, хакерлер ықтимал пайдаланушы аттарының (логиндердің) тізімін және ықтимал парольдердің тізімін оңай құрастырып, оларды компьютерлердің ең қол жетімді санына сәйкестендіретін бағдарламаны іске қоса алады. Ұқсас зерттеулер IOActive-де 2013 жылдың наурыз айында жүргізілді. Үйдегі маршрутизаторлар мен приставкалардың ұзақ тізімі олардың осалдығын қарапайым бұзылулардан анықтау үшін сканерленді.

Көптеген пайдаланушы аттары мен парольдерді қолдануға тырысудың орнына, олар өндірушілер орнатқан бір ғана танымал логин мен парольді қолданып көрді деп болжауға болады. Пайдаланушылар бұл мәндерді бірден өзгертеді деп болжалды, бірақ көбісі бұлай жасамағаны белгілі болды. Зерттеушілер жүздеген мың ұқсас құрылғылардың ықтимал осалдығын анықтады. Ирандық ядролық объектіге Stuxnet-шабуыл кезінде бұзушылар центрифугаларды басқаратын Siemens компьютерлерінде жылдар бойы Интернетте айналып келе жатқан әдепкі парольдердің бірін қолданғанын пайдаланып, одан да алаңдатарлық жағдай деп санауға болады. Бүкіләлемдік ғаламтордың танымалдылығының артуы мәселені одан әрі қиындатты.

Бір парольдің орнына, қазір көптеген адамдарда он немесе оданда көп нәрсе бар. Барлық осы құпия сөздерді есте сақтау өте қиын болғандықтан, адамдар

қарапайым, тұрақсыз парольді алып, оны көптеген веб-сайттарда қолдануға тырысады (Флоренсио және Герли, 2007; Gaw and Felten, 2006). Құпия сөздерді табуоңай деп қорқудың қажеті бар ма? Әрине, тұрарлық. 1998 жылы San Jose Mercury News Беркли қаласының тұрғыны Питер Шипли бірнеше компьютерлерді бір коммутатордың барлық 10 000 нөміріне (мысалы, (415) 7700xxxx) қоңырау шалған автокөлік қоңырау құрылғысы ретінде қолданғанын, телефон компанияларын алдау үшін нөмірлерді кездейсоқ сұрыптап, компьютерлердің осындай қолданылуына кедергі келтіріп, осы әрекеттерді анықтауға тырысқанын хабарлады. 2,6 миллион қоңырау шалғаннан кейін, Шипли шығанағы аймағында 20000 компьютерді тапты, олардың 200-інде қорғаныс жоқ.

Оның айтуынша, тұрақты крекер басқа адамдардыңкомпьютерлерінің 75% - ына ене алады (Деннинг, 1999). Бірақ мұның бәрі ежелгі уақытқа оралу болды, өйткені компьютер 2,6 миллион телефон нөміріне қоңырау шалуы керек еді. Хакерлер тек Калифорнияда ғана емес. Австралиялық крекер дәл осылай жасауға тырысты. Ол бұзған жүйелердің ішінде Сауд Арабиясындағы Citibank компьютері болды, оған несие карталарының нөмірлері мен несие лимиттері туралы ақпарат (бір жағдайда — 5 миллион доллар), сондай-ақ транзакциялар туралы жазбалар (оның ішінде қоғамдық үйге бару үшін кем дегенде бір аударым) алуға мүмкіндік берді.

Оның әріптесі, сонымен қатар банк жүйесіне еніп, 4000 несие картасының нөмірін жинады (Деннинг, 1999). Мұндай ақпарат мақсатсыз пайдаланылған кезде, банк клиент жария етуге тиіс деп мәлімдей отырып, өз қатесінің мүмкіндігін сөзсіз және батыл түрде жоққа шығарады. Интернет хакерлер үшін нағыз сыйлық болды. Ол исключил все алғанда, олардың жұмыс. Ендікейбір телефон нөмірлеріне қоңырау шалудың қажеті жоқ. Қоңырау келесі рәсімге айналды. Хакер IP-мекен-жайлар жиынтығы бойынша пинг сұрауларын (желілік пакеттер) жіберетін сценарий жаза алады.

Егер ол қандай-да бір жауап алса, содан кейін сценарий TCP қосылымын машинада іске қосылуы мүмкін барлық қызметтерге орнатуға тырысты. Жоғарыда айтылғандай, портты сканерлеу деп аталатын және сценарийді нөлден жазудың орнына, крекер Nmap сияқты мамандандырылған құралдарды қолдана алады, бұл кеңейтілген портты сканерлеу технологиясының кең спектрін ұсынады. Алайын, қандай қызмет, қай машинада іске қосылған взломщик еді кірісуге шабуыл. Мысалы, егер крекер құпия сөзді қорғауды зерттегісі келсе, ол осы аутентификация әдісін қолданған қызметтерге, мысалы, telnet серверіне немесе тіпті веб-серверге қосылуы керек еді. Біз әдепкі пароль немесе бір немесе басқа тұрақсыз пароль бұзушыларға көптеген есептік жазбалардан, кейде тіпті толық әкімшілік құқықтармен егін жинауға мүмкіндік беретінін көрдік.

Unix-тегі құпия сөзді қорғау. Кейбір ескірген операциялық жүйелерде парольдер дискіде шифрланбаған түрде сақталды, бірақ әдеттегі жүйелік қорғаныс механизмдері арқылы қорғалды. Дискідегі барлық құпия сөздерді шифрланбаған түрде сақтау біршама қиындық тудырды, өйткені көптеген

адамдар оларға қол жеткізе алды. Оларға жүйелік әкімшілер, машина операторлары, қызметкерлер,бағдарламашылар, менеджерлер және тіпті кейбір хатшылар кіруі мүмкін. UNIX-тесәтті шешім қолданылады.

Кіру бағдарламасы Пайдаланушыдан оның аты мен паролін енгізуді сұрайды. Пароль дереу" шифрланған", оны бекітілген деректер блогын шифрлау кілті ретінде пайдалану арқылы. Шын мәнінде, кіріс ретінде парольмен және шығыс ретінде парольмен бір жақты функция іске қосылады. Бұл процесс нақты шифрлау емес, бірақ оны шифрлау деп атау оңайырақ. Содан кейін кіру бағдарламасы ASCII жолдарының қарапайым жиынтығы болып табылатын құпия сөз файлын оқиды, әр пайдаланушы үшін біреуі тіркеу аты бар жолды тапқанша. Егер осы жолдағы шифрланған пароль тек есептелген шифрланған парольге сәйкес келсе, кіруге рұқсат етіледі, ал егер сәйкес келмесе, ол қабылданбайды.

Бұл схеманың артықшылығы-ешкім, тіпті артықшылықты қолданушы да құпия сөздерді таба алмайды, өйткені олар жүйеде шифрланбаған түрде сақталмайды. Иллюстрация үшін біз қазір шифрланған пароль пароль өрісінде сақталады делік. Кейінірек біз UNIX-тің қазіргі нұсқаларында бұл енді жасалмайтынын көреміз. Егер крекер шифрланған парольді ала алса, схема келесі шабуылға ұшырауы мүмкін. Алдымен крекер Моррис пен Томпсон сияқты мүмкін парольдердің сөздігін жасайды.

Олар белгілі алгоритмді қолдана отырып алдын-ала шифрланған. Бұл процесс қанша уақытқа созылатыны маңызды емес, өйткені ол бұзылуға тырысқанға дейін де жүреді. Енді парольдер мен шифрланған парольдердің тізімімен қаруланған крекер соққы береді. Ол жалпыға қол жетімді пароль файлын оқиды және одан барлық шифрланған парольдерді шығарады.

Бұл парольдер оның тізіміндегі шифрланған парольдермен салыстырылады. Әр сәйкестікте тіркеу аты және шифрланбаған пароль белгілі болады. Қабықта жұмыс істейтін қарапайым сценарий бұл процесті автоматтандырады және оны бірнеше секунд ішінде жасауға болады.

Сценарийді қалыпты іске қосу арқылы сіз ондаған парольдерді ала аласыз. Мұндай шабуылдың мүмкіндігін түсінген Моррис пенТомпсон шабуылды іс жүзінде пайдасыз ететін технологияны сипаттады. Идея әр парольмен тұз (тұз) деп аталатын N-биттік кездейсоқ санды байланыстыру болды. Кездейсоқ Сан парольдің әр өзгеруімен өзгереді. Ол құпия сөз файлындашифрланбаған түрде сақталады және оны кез-келген адам оқи алады.

Шифрланған парольді пароль файлында сақтаудың орнына, алдымен пароль мен кездейсоқ Сан біріктіріліп, содан кейін бірге шифрланады. Алынған шифрланған нәтиже пароль файлында сақталады. 16-сурет бес қолданушыға арналған пароль файлын көрсетеді:Bobbie, Tony, Laura, Mark және Deborah. Файлдағы әр пайдаланушыға үтірменбөлінген үш жазбадан тұратын бір жол бөлінген: тіркеу атауы, тұз және "пароль + тұз"шифрланған тіркесімі. E(Dog, 4238) жазбасы Bobbie-ге тиесілі Dog паролін кездейсоқ тағайындалған 4238 тұзымен біріктірудің және оларды е шифрлау функциясы арқылы өткізудің нәтижесін білдіреді.

Енді ықтимал парольдердің тізімін жасап, оларды шифрлап, нәтижелерін сұрыпталған f файлында сақтағысы келетін крекер үшін Бұл не болатынын көрейік, осылайша әр шифрланған парольді оңай табуға болады. Егер шабуылдаушы парольDog сөзі болуы мүмкін деп болжаса, енді Dog-ны шифрлау және нәтижені F файлынақою жеткіліксіз. ол Dog0000, Dog0001, Dog0002 және т. б.сияқты 2n жолдарын цифрлап, осы жолдардың барлығын F файлына енгізуі керек. UNIX жүйесінде бұл әдіс n = 12 көмегімен қолданылады. Қосымша қорғаныс үшін UNIX-тің кейбір заманауи нұсқаларында шифрланған парольдер, әдетте, жеке "көлеңкелі" файлда сақталады, оны пароль файлынан айырмашылығы тек түбірлік пайдаланушы оқи алады. Пароль файлына тұз қосып, оны оқылмайтын етіп өзгерту, жанама (және баяу) оқуды қоспағанда, осы файлға қатысты көптеген шабуылдарға төтеп бере алады.

Bobbie,4238, e(Dog,4238)
Tony,2918,e(6%%TaeFF,2918)
Laura,6902, e(Shakespeare,6902)
Mark,1694,e(XaB#Bwcz,1694)
Deborah, 1092, e(LordByron,1092)

2-сурет. Шифрланған парольдерді алдын-ала есептеу үшін тұзды пайдалану

Бір реттік парольдер. Артықшылықты пайдаланушылардың көпшілігі қарапайым адамдарды айына бір рет құпия сөздерін өзгертуге көндіреді. Бірақ, оларға ешкім ескертулерін қабылдай алады. Жүйеге кірген сайын парольді өзгерту одан да экстремалды болып көрінеді, бұл бір реттік парольдерді (one-time passwords) пайдалануға әкеледі. Мұндай парольдерді пайдаланған кезде пайдаланушы парольдер тізімі бар блокнот алады. Жүйеге кірген сайын тізімдегі келесі пароль қолданылады. Хакер парольді тапса да, оны пайдалана алмайды, өйткені келесі

жолы басқа парольді пайдалану керек болады. Бұл жағдайда пайдаланушы пароль дәптерін жоғалтпауы керек.

Шын мәнінде, Лесли Лампорт ойлап тапқан (Lamport, 1981) қолданушыға бір реттік парольдерді қолдана отырып, қауіпті желі арқылы қауіпсіз кіруді қамтамасыз ететін талғампаз схеманың арқасында сіз осындай блокнотсыз жасай аласыз. Лэмпорт әдісін үйдегі жеке компьютерде жұмыс істейтін қолданушы интернет арқылы серверге кіру үшін қолдана алады, тіпті хакерлер барлық трафикті екі бағытта да қадағалап, көшіре алады. Сонымен қатар, файлдық жүйелерде серверде де, пайдаланушының үй компьютерінде де ешқандай құпияны сақтаудың қажеті жоқ. Кейде бұл әдіс бір жақты хэш тізбегі деп аталады (one-way hash chain). Алгоритм бір жақты функцияға, яғни y = f(x) функциясына негізделген, ол x болғанкезде y-ны оңай алуға мүмкіндік беретін қасиетке ие. Кіріс және шығыс бірдей ұзындықта болуы керек, мысалы, 256 бит. Пайдаланушы есте сақтау керек құпия сөзді таңдайды. Ол сонымен қатар алгоритм құра алатын бір реттік парольдер санына сәйкес келетін N бүтін санды

таңдайды. Мысалы, N = 4 — ті қарастырайық,бірақ іс жүзінде әлдеқайда үлкен мән қолданылуы керек N. егер құпия пароль s болса, онда бірінші пароль бір жақты функцияны N рет іске қосу арқылы алынады: P1 = F(F(F(F(s))) екінші пароль бір жақты функцияны (n – 1) рет іске қосу арқылы алынады: P2 = f(f(F(s))) үшінші парольді алу үшін f функциясы екі рет, ал төртінші парольді алу үшін — бір рет. Жалпы алғанда, Pi -1 = f(Pi). Мұнда бастысы, егер осы тізбектегі кез-келген пароль болса, оған тиесілі алдыңғы парольді есептеу қиын емес, бірақ келесі парольді есептеу мүмкін емес екенін түсіну. Мысалы, P2 болса, P1табу қиын емес, бірақ P3 табу мүмкін емес. Сервер P0 санымен іске қосылады, ол f(P1).

Бұл мән пайдаланушының тіркеу атымен байланысты пароль файлының жазбасында сақталады, сонымен бірге 1 бүтін санмен бірге келесі P1 паролі талап етілетінін көрсетеді. Пайдаланушы бірінші рет кіргісі келгенде, ол өзінің тіркеу атауын пароль файлындағы 1 бүтін санды жіберу арқылы жауап беретін серверге жібереді. Пайдаланушы машинасы жауап ретінде P1 жібереді, оны жергілікті жердетерілген s мәнінен есептеуге болады. Содан кейін сервер f(P1) есептейді және алынған мәнді пароль файлында (P0) сақталған мәнмен салыстырады. Егер мәндер сәйкес келсе, кіруге рұқсат етіледі, бүтін сан 2-ге дейін артады, ал пароль файлындағы P0 мәні P1 мәніне сәйкес келеді. Келесі кіру кезінде сервер пайдаланушыға 2 санын жібереді, ал пайдаланушы машинасы P2 паролін есептейді. Содан кейін сервер f(P2) есептейді және алынған мәнді пароль файлындағы жазбамен салыстырады. Егер мәндер сәйкес келсе, кіруге рұқсат етіледі, бүтін сан 3-ке дейін артады, ал пароль файлындағы P2 паролі P1 паролінің үстіне жазылады. Бұл схеманың жұмыс істеуіне мүмкіндік беретін қасиет , егер крекер Pi-ді ұстап алса да,одан Pi + 1 мәнін есептеу мүмкіндігі болмайды, ол тек Pi -1 паролінің мәнін есептейалады, ол бұрын қолданылған және ешқандай құндылықты білдірмейді. Барлық n парольдер қолданылған кезде, сервер жаңа құпия кілтпен қайта іске қосылады.

Ұсынылған әдебиеттер:

Негізгі әдебиеттер:

1. Нестеров, С. А. Основы информационной безопасности: учебник для вузов/ С. А. Нестеров. - Санкт-Петербург : Лань, 2021., 324 с. — ISBN 978-5-8114-6738-9.

2. Зенков, А. В. Информационная безопасность и защита информации: учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2023. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9

3. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3

Қосымша әдебиеттер:

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Высшее образование). — ISBN 978-5-534- 07248-8

2. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2023. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1

3. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2023. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0