ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
«Ғ.ДАУКЕЕВ АТЫНДАҒЫ АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ»
коммерциялық емес акционерлік қоғамы
Телекоммуникациялық желілер және жүйелер кафедрасы

«ҚОРҒАУҒА ЖІБЕРІЛДІ»
Кафедра меңгерушісі Темырканова Э.К
(ғылыми дәрежесі, атағы, Т.А.Ж.)
_____ «____» _____2020ж.
(қолы)

ДИПЛОМДЫҚ ЖОБА

Тақырыбы: Байланыс желілеріндегі ақпараттық қауіпсіздік әдістерін талдау
Мамандығы 5В071900 Радиотехника, электроника және телекоммуникациялар
Орындаған Тулен Бекнұр Шукурханұлы Тобы РЭТ(ИКТ)-16-1
(Т.А.Ж.)
Ғылыми жетекшісі PhD-доктор, доцент Чайко Е.В.
(ғылыми дәрежесі, атағы, Т.А.Ж.)
Кеңесшілер:
экономикалық бөлім бойынша:
доцент Тузелбаев Бакберген Ибадиллаевич
(ғылыми дәрежесі, атағы, Т.А.Ж.)
_____ «_09___» __05_____2020ж.
(қолы)
өміртіршілігі қауіпсіздігі бойынша:
доцент Жандаулетова Фарида Рустембековна
(ғылыми дәрежесі, атағы, Т.А.Ж.)
_____ «_21___» _____05_____2020ж.
негізгі бөлім бойынша:
аға оқыт. Балгабекова Ляйлим Озбековна
(ғылыми дәрежесі, атағы, Т.А.Ж.)
_____ «__27__» _____05_____2020ж.
(қолы)
есептеу техникасын қолдану бойынша:
аға оқыт. Балгабекова Ляйлим Озбековна
(ғылыми дәрежесі, атағы, Т.А.Ж.)
_____ «_29___» _____05_____2020ж.
(қолы)
Нормобақылаушы: Мухамеджанова Альмира Далелханкызы
(ғылыми дәрежесі, атағы, Т.А.Ж.)
_____ «_09___» _____06_____2020ж.
(қолы)
Пікір беруші: _____
(ғылыми дәрежесі, атағы, Т.А.Ж.)
_____ «____» _____2020ж.
(қолы)

Алматы 2020

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
«Ғ.ДАУКЕЕВ АТЫНДАҒЫ АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ»
коммерциялық емес акционерлік қоғамы

Ғарыштық инженерия және телекоммуникация институты

Телекоммуникациялық желілер және жүйелер кафедрасы

Мамандығы 5В071900 – Радиотехника, электроника және телекоммуникациялар

Дипломдық жобаны орындауға берілген

ТАПСЫРМА

Студент Тулен Бекнұр Шукурханұлы
(Т.А.Ж.)

Жобаның тақырыбы Байланыс желілеріндегі ақпараттық қауіпсіздік әдістерін талдау

2019_ ж. «_11_» __11____ № 147_университет бұйрығымен бекітілді.

Аяқталған жобаны тапсыру мерзімі «__29_»___05_____2020___ж.

Жобаға алғашқы деректер (талап етілетін зерттеу (жоба) нәтижелерінің параметрлері және зерттеу нысанының алғашқы деректері):
1 Байланыс желілеріндегі ақпаратқа мүмкін болар қауіп көздерін саралау____
2 Ақпараттық қауіпсіздікте қолданылатын әдістер мен құралдарына анализ жасау_____
3 IPS жүйесін қарастыру_____

Диплом жобасындағы әзірленуі тиіс мәселелер тізімі немесе диплом жобасының қысқаша мазмұны:
Кіріспе_____
1 Қазіргі заманғы желінің қауіпсіздік қатерлері _____
2 Желіні қорғау әдістері_____
3 IPS жүйесін конфигурациялау_____
4 Тіршілік қауіпсіздігі _____
5 Экономикалық бөлім_____
Қорытынды_____
Әдебиеттер тізімі_____
_____
_____
_____
_____
_____

Графикалық материалдардың (міндетті түрде дайындалатын сызбаларды көрсету) тізімі:

Шабуыл құралдарының күрделілігі vs. қажетті техникалық білім

Желілерге қауіп

Шифрлау арқылы құпиялылық

Пакет сниффері мысалы

Пинг-свип мысалы

Zero-Day Exploit шабуылы

IPS сенсорды орналастыру мысалы

Қарапайым LAND шабуылын басып алу

CCO сигнатура файлдары

SSH сеансының Follow TCP Stream терезесі

Syslog серверіндегі логтар журналы

IPS ережелерін қолданнан кейінгі портты сканерлеу нәтижесі

Негізгі ұсынылатын әдебиеттер:

1 N. Fisk. Malware Incidents // Encyclopedia of Cybercrime / Samuel C. McQuade, III. — London : Greenwood Press, 2009. — P. 124. — ISBN 978-0-313-33974-5.

2 Anderson, James P., "Computer Security Threat Monitoring and Surveillance, " Washing, PA, James P. Anderson Co.,1980.

3 Ж.С. Абдимуратов. Охрана труда. Методические указания к выполнению расчетно-графических работ для студентов - бакалавров специальности 5В071800- «Электроэнергетика» - Алматы: АУЭС, 2013 - 22с.

4 Методические указания для экономической части выпускной работы составители: Базылов К. Б.,Алибаева С. А.,Бабич А. А.- АИЭС.- 2008г.

Жоба бойынша жобаның бөлімдеріне қатысты белгіленген кеңесшілер

Бөлімдері	Кеңесшілері	Мерзімі	Қолы
Экономика	Тузелбаев Б.И.	09.05.20	
Ө.Т.Қ.Н.	Жандаулетова Ф.Р.	21.05.20	
Негізгі бөлім	Балгабекова Л.О.	27.05.20	
Есептеу техникасы	Балгабекова Л.О.	29.05.20	
Нормабақылау	Мухамеджанова А.Д.	09.06.20	

Диплом жобасын дайындау

КЕСТЕСІ

Бөлімдердің атауы, әзірленетін мәселелердің тізімі	Ғылыми жетекшіге ұсыну мерзімдері	Ескерту
1. Кіріспе	03.03.20	
2 Қазіргі заманғы желінің қауіпсіздік қатерлері	10.03.20	
3 Желілік қауіпсіздік құралдарының эволюциясы	15.03.20	
4 Желілік қауіптер	21.03.20	
5 Шифрлау және криптография	28.03.20	
6 Желіні қорғау әдістері	02.04.20	
7 Желі шабуылдарын жұмсарту	09.04.20	
8 IPS системасы	16.04.20	
9 IPS сигнатуралары	25.04.20	
10 IPS жүйесін конфигурациялау	01.05.20	
11 Тіршілік қауіпсіздігі	21.05.20	
12 Экономикалық бөлім	09.05.20	
13 Қорытынды	01.06.20	

Тапсырманың берілген уақыты «_17__» __ақпан_____2020___ж.

Кафедра меңгерушісі _____ (Темырканова Эльвира Кадылбековна)
(қолы) (Т.А.Ж.)

Жобаның
ғылыми жетекшісі _____(Чайко Елена Валерьевна)
(қолы) (Т.А.Ж.)

Орындалатын тапсырманы
қабылдаған студент _____ (Тулен Бекнұр Шукурханұлы)
(қолы) (Т.А.Ж.)

Аңдатпа

Бұл дипломдық жұмыста байланыс желілеріндегі ықтимал қауіптер мен шабуылдарды зерттеу және олардың алдын алу әдістері қарастырылған. Қазіргі желідегі белгілі шабуылдар мен қауіптерге толықтай талдау жүргізілген. Сонымен қатар еңбекті қорғау бойынша қауіпті және зиян өндірістік факторлармен қорғау шараларын талдау сұрақтары қарастырылған. Экономикалық бөлімінде жүйені жобалауға және енгізіп іске асыру шығындар мен кірістерге есептеу жүргізілен.

Аннотация

В данной дипломной работе предусмотрены методы исследования и предотвращения возможных угроз и атак в сетях связи. Проведен полный анализ известных атак и угроз в современной сети. Кроме того, рассмотрены вопросы анализа мероприятий по охране труда с опасными и вредными производственными факторами. В экономической части производится расчет затрат и доходов на проектирование и внедрение системы.

Abstract

This thesis provides methods of research and prevention of possible threats and attacks in communication networks. A complete analysis of known attacks and threats in the modern network. In addition, the issues of analysis of measures on labor protection with hazardous and harmful production factors. In the economic part of the calculation of costs and revenues for the design and implementation of the system.

Мазмұны

Кіріспе

Желілік қауіпсіздік қазір компьютерлік желілердің ажырамас бөлігі болып табылады. Желілік қауіпсіздік протоколдарды, технологияларды, құрылғыларды, деректерді қорғаудың және қауіптерді төмендетудің құралдары мен әдістерін қамтиды. Желілік қауіпсіздік шешімдері 1960 жылдары пайда болды, бірақ 2000-шы жылдарға дейін. олар қазіргі заманғы желілердің кешенді шешімдеріне айналған жоқ.

Желілік қауіпсіздік көбінесе зиянды хакерлерден бір сатыға қалғысы келеді. Дәрігерлер жаңа аурудың бар проблемаларды емдеуге жол бермейтіні сияқты, желілік қауіпсіздік мамандары нақты уақыттағы шабуылдардың әсерін азайту арқылы ықтимал шабуылдардың алдын алуға тырысады. Бизнестің үздіксіздігі желі қауіпсіздігінің тағы бір маңызды факторы болып табылады. Желілік қауіпсіздік ұйымдары желілік қауіпсіздік мамандарының ресми қауымдастықтарын құру үшін құрылды. Бұл ұйымдар стандарттар орнатады, ынтымақтастықты ынталандырады және желінің қауіпсіздігі саласындағы мамандарға персоналды дамыту мүмкіндіктерін ұсынады. Желілік қауіпсіздік мамандары осы ұйымдар беретін ресурстар туралы білуі керек. Желілік қауіпсіздіктің күрделілігі оны қамтитын барлық нәрсені игеруді қиындатады. Әр түрлі ұйымдар желінің қауіпсіздігі әлемін басқарылатын бөліктерге бөлетін домендер құрды. Бұл бөлу кәсіпқойларға оқыту, зерттеу және жұмысқа орналасудың нақты бағыттарына назар аударуға мүмкіндік береді. Желілік қауіпсіздік саясатын қызметкерлер мен олардың күнделікті жұмысы кезінде басшылыққа алу үшін компаниялар мен мемлекеттік ұйымдар жасайды. Басқару деңгейіндегі желілік қауіпсіздік мамандары желі қауіпсіздігі саясатын жасауға және жүргізуге жауап береді. Желілік қауіпсіздіктің барлық әдістері желінің қауіпсіздік саясатымен байланысты және басшылыққа алынады.

Желілік қауіпсіздік желілік қауіпсіздік домендерінен тұратындықтан, желілік шабуылдар оларды оңай тануға және дұрыс қарауға болатындай етіп жіктеледі. Вирустар, құрттар және трояндық аттар - бұл желілік шабуылдардың ерекше түрлері. Жалпы алғанда, желілік шабуылдар барлау, қол жеткізу немесе қызмет көрсетуден бас тарту ретінде жіктеледі (DoS).

Желілік шабуылдардың салдарын азайту - желілік қауіпсіздік маманының жұмысы. Бұл дипломдық жұмыста желілік шабуылдарды болдырмау әдістері талданады.

1 Қазіргі заманғы желінің қауіпсіздік қатерлері

1.1 Желілік қауіпсіздік құралдарының эволюциясы

2001 жылдың шілдесінде Code Red Worm бүкіл әлемдегі веб-серверлерге шабуыл жасап, 350 000-нан астам хостты жұқтырды. Ол электрондық поштаны немесе тарату үшін қолданбалы файлдарды жұқтырған жоқ. Жаңа компьютерді жұқтыру арқылы құрт өзінің 100 клонын құрды, олардың әрқайсысы Microsoft IIS веб-серверінің осалдықтары арқылы таратудың жаңа мақсаттарын іздей бастады [1]. Code Red Worm миллиондаған қолданушыларға қызмет көрсетілуіне бас тартты.

Егер осы Code Red-пен зарарланған серверлерге жауап беретін желілік қауіпсіздік мамандары уақытында қауіпсіздік саясатын жасап, жүзеге асырғанда, қауіпсіздік түзетулері дер кезінде қолданылатын еді. Code Red Worm тоқтатылып, желінің қауіпсіздігі тарихында тек ескертпе ретінде қалар еді.

Желілік қауіпсіздік ұйымның үздіксіз жұмысымен тікелей байланысты. Желілік қауіпсіздіктегі олқылықтар электронды сауданы бұзуы мүмкін, іскери деректердің жоғалуына әкелуі мүмкін, адамдардың жеке өміріне қауіп төндіреді және ақпараттың тұтастығын бұзады. Бұл бұзушылықтар корпоративті кірістің жоғалуына, зияткерлік меншіктің ұрлануы мен сот процестеріне әкелуі мүмкін, тіпті қоғамдық қауіпсіздікке қауіп төндіруі мүмкін.

Қауіпсіз желіні қолдау желіні пайдаланушылардың қауіпсіздігін қамтамасыз етеді және коммерциялық мүдделерін қорғайды. Желілік қауіпсіздікті сақтау ұйымның желілік қауіпсіздік сарапшыларының мұқият болуын талап етеді. Желілік қауіпсіздік мамандары жаңа және пайда болатын қауіптер мен желілерге шабуылдар, сонымен қатар құрылғылар мен қосымшалардың осалдықтары туралы хабардар болуы керек. Бұл ақпарат шабуылдардың алдын-алу әдістерін бейімдеу, дамыту және енгізу үшін қолданылады. Алайда, желінің қауіпсіздігі, сайып келгенде, оны пайдаланатындардың барлығына жүктеледі. Осы себепті, желілік қауіпсіздік маманының міндеті - барлық қолданушыларға қауіпсіздік бойынша оқытудан өту. Қауіпсіз, қауіпсіз желіні ұстау барлығына тұрақты, функционалды жұмыс ортасын қамтамасыз етеді.

«Қажеттілік - өнертабыстың анасы». Бұл сөз желінің қауіпсіздігі үшін өте жақсы. Интернеттің алғашқы күндерінде коммерциялық мүдделер мардымсыз болды. Интернетте ешқандай қауіпсіздік шаралары болған жоқ, бірақ ертерек пайдаланушылар басқа пайдаланушыларға зиян келтіретін әрекеттерді сирек жүргізетін.

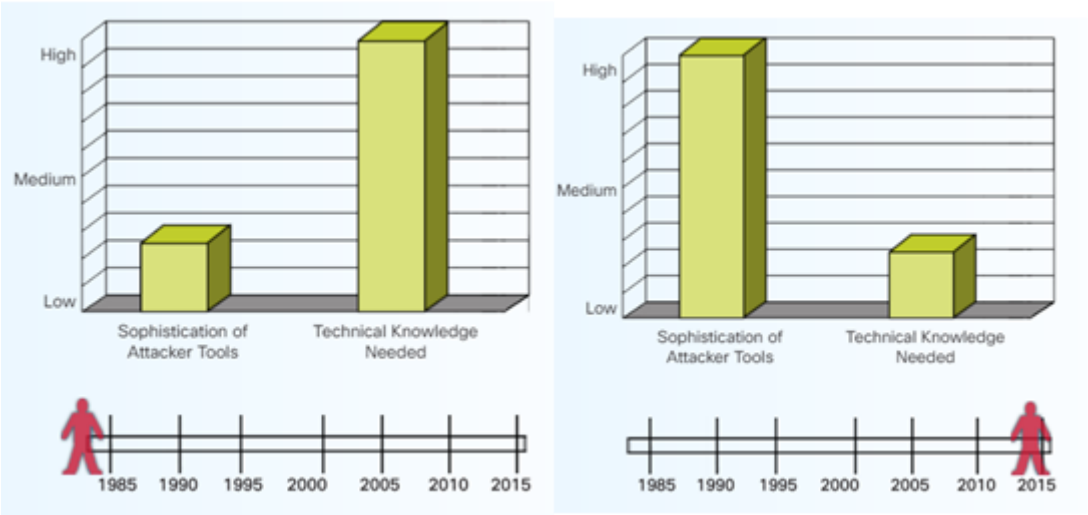
Алғашқы кезеңдерде желі қызметі адамдар мен машиналарды байланыс құралдары арқылы байланыстырды. Желілік желінің жұмысы пайдаланушының ақпарат пен идеяларды беру қабілетін жақсарту үшін құрылғыларды қосу болды. Ерте Интернет қолданушылары өздерінің желілік

белсенділігі желіге немесе өз деректеріне қауіп төндіретіні туралы ойлануға көп уақыт жұмсамады.

Алғашқы вирустар шығарылып, алғашқы DoS шабуылы орын алғанда, желі мамандарында өзгерістер басталды. Пайдаланушылардың қажеттіліктерін қанағаттандыру үшін желі мамандары желілерді қорғауды үйренді. Көптеген желілік мамандардың назары желілерді жобалау, құру және өсуден қолданыстағы желілерді қорғауға көшті.

Бүгінгі таңда Интернет - оның шығу тегіне қарағанда мүлде басқа желі. Көптеген адамдар желіге жеке, қаржылық және іскери қажеттіліктері үшін жүгінеді. Бұл ақпарат қорғалуы керек. Алайда, шабуыл құралдары әлдеқайда күрделі және жоғары автоматтандырылған, сондықтан оларды қолдану бұрынғыдан гөрі аз техникалық білімді қажет етеді (1.1 сурет).

Желілік қауіпсіздік бойынша маманның жұмысы тиісті қызметкерлердің желілік қауіпсіздік құралдарын, процестерін, әдістерін, хаттамаларын және технологияларын жақсы білуді қамтамасыз етеді. Желілік қауіпсіздік мамандары желілерге туындайтын қауіптерді басқаруы өте маңызды.



1.1 сурет – Шабуыл құралдарының күрделілігі vs. қажетті техникалық білім

Желілік қауіпсіздік күнделікті жұмыстың ажырамас бөлігі болғандықтан, желінің қауіпсіздігін қамтамасыз ететін белгілі бір функцияларды орындайтын құрылғылар пайда болды.

Алғашқы желілік қауіпсіздік құралдарының бірі 1984 жылы SRI International компаниясы жасаған интрузияны анықтау жүйесі (IDS) болды [2]. IDS нақты уақыт режимінде шабуылдардың белгілі бір түрлерін анықтай алады. Бұл желілік қауіпсіздік мамандарына осы шабуылдардың желілік құрылғылар мен пайдаланушыларға теріс әсерін тезірек азайтуға мүмкіндік береді. 1990 жылдардың соңында IDS шешімі интрузияның алдын-алу

жүйесімен (IPS) ауыстырылды. IPS құрылғылары зиянды әрекетті анықтай алады және нақты уақытта шабуылды автоматты түрде блоктай алады.

IDS және IPS шешімдеріне қосымша, қажетсіз трафиктің желінің белгіленген аумағына кіруін болдырмайтын, сол арқылы периметрдің қауіпсіздігін қамтамасыз ететін желілік экран жасалынған. 1988 жылы Digital Equipment Corporation (DEC) пакеттік сүзгі формасындағы бірінші желілік экран жасады. Бұл алғашқы желілік экрандар пакеттерді алдын-ала белгіленген ережелер жиынтығына сәйкес тексеріп, пакеттерді сәйкесінше жіберуге немесе тастауға болатын мүмкіндіктерге ие болды. 1989 жылы AT&T Bell Laboratories алғашқы күйі сақталынатын желілік экранды жасады [3]. Пакеттік сүзгі желілік экраны сияқты, қосылуға арналған желіаралық қалқан трафикке рұқсат беру немесе бұғаттау үшін алдын-ала белгіленген ережелерді қолданады. Пакеттік сүзгі желілік экранының айырмашылығы, қосылу күйіндегі желілік экранды орнатылған байланыстарды бақылайды және пакеттің деректердің ағымына жататынын анықтайды, бұл үлкен қауіпсіздікті және жылдам өңдеуді қамтамасыз етеді.

Түпнұсқалық желілік экран маршрутизаторлар сияқты желілік құрылғыларға қосылған бағдарламалық жасақтама мүмкіндіктері болды. Уақыт өте келе, бірнеше компания маршрутизаторлар мен қосқыштарға жадты және сүзгі пакеттерінің процессорлық жүктемелерін түсіруге мүмкіндік беретін жеке немесе арнайы жасады. Cisco адаптивті қауіпсіздік құралы (ASA) контекстке негізделген жеке желілік экран ретінде қол жетімді. Арнайы желілік экранды қажет етпейтін ұйымдар үшін Cisco Integrated Services Router (ISR) сияқты заманауи маршрутизаторларды қосылудың күрделі күйінде қалқан ретінде пайдалануға болады.

Дәстүрлі қауіпсіздік көп қабатты өнімдерге және бірнеше сүзгілерді пайдалануға негізделген. Алайда, қауіптер күрделене түскен сайын, бұл сүзгілер желілік және қолданбалы деңгейдегі трафикті тереңірек талдау үшін қажет болды. Қауіпсіздік талаптары ақпараттың динамикалық жаңартылуын және қауіптерге тезірек жауап беруді қамтыды. Осы себепті, Cisco қауіпсіздік барлау операцияларын (SIO) жасады. SIO - бұл ғаламдық қатерлер туралы ақпаратты, беделге негізделген қызметтерді және Cisco желілік қауіпсіздік құралдарымен күрделі талдауды жылдам жауап беру уақытында сенімді қорғауды қамтамасыз ететін бұлтқа негізделген қызмет.

Желілік қауіпсіздік құралдарының эволюциясы:

- 1988, DEC Packet Filter Firewall;
- 1989, AT&T Bell Labs Stateful Firewall;
- 1991, DEC SEAL Application Layer Firewall;
- 1994, Check Point Firewall;
- 1995, NetRanger IDS;
- 1997, RealSecure IDS;
- 1998, Snort IDS;
- 1996, First IPS;
- 2006, Cisco Zone-Based Policy Firewall;

- 2010, Cisco Security Intelligence Operations.

1.2 Желілік қауіптер

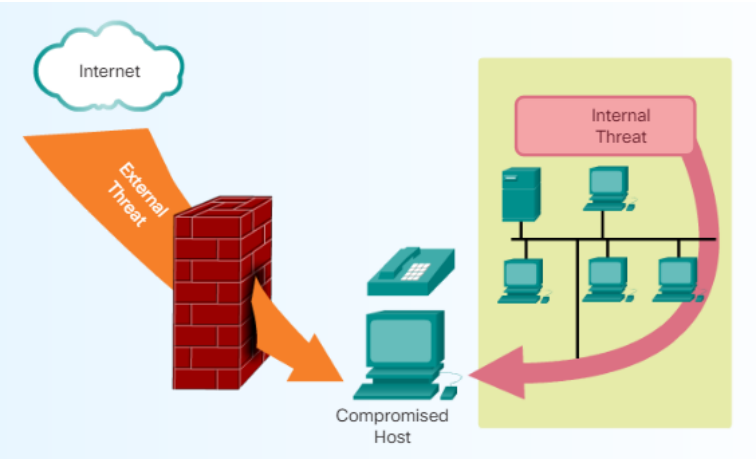
1.2 суретте көрсетілгендей, желіден тыс қауіптермен жұмыс істеумен қатар, желінің қауіпсіздігі бойынша сарапшылар желі ішіндегі қауіптерге де дайын болуы керек. Ішкі қауіптер, қасақана немесе кездейсоқ болсын, корпоративті желі мен деректерге тікелей қол жетімділік пен білімнің арқасында сыртқы қауіптен гөрі көбірек зиян келтіруі мүмкін. Осыған қарамастан, ішкі қауіптерді азайту құралдары мен әдістерін жасау үшін сыртқы қатерлерді азайтуға арналған құралдар мен әдістер енгізілгеннен кейін 20 жылдан астам уақыт өтті.

Желінің ішінен шығатын қауіп-қатердің жалпы сценарийі - бұл белгілі бір техникалық дағдылары бар және зиян келтіруге дайын болған ашуланған қызметкер. Желі ішіндегі қауіптердің көпшілігі жергілікті желіде (LAN) немесе коммутация инфрақұрылымында қолданылатын протоколдар мен технологияларды қолданады. Бұл ішкі қауіптер екі санатқа бөлінеді: спуфинг және DoS.

Спуфингтік шабуылдар дегеніміз - бір құрылғы деректерді жалған жасау арқылы екіншісін өзгертуге тырысатын шабуылдар. Спуфингтік шабуылдардың бірнеше түрі бар. Мысалы, MAC мекен-жайын бұзу бір компьютер басқа компьютердің MAC адресі негізінде деректер пакеттерін қабылдаған кезде пайда болады.

DoS шабуылдары компьютерлік ресурстарды пайдаланушылар үшін қол жетімді етпейді. Зиянкестер DoS шабуылдарын жүргізу үшін әртүрлі әдістерді қолданады.

Желілік қауіпсіздік саласындағы кәсіпқой ретінде, қауіптердің осы түрлерімен күресу және жергілікті желінің қауіпсіздігін қамтамасыз ету үшін арнайы әзірленген әдістерді түсіну маңызды.



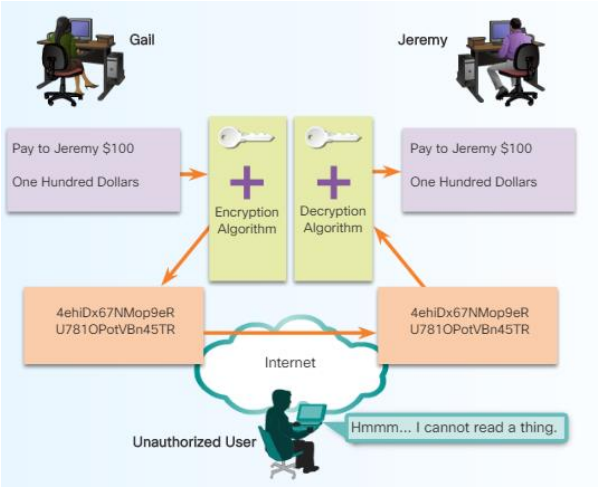
1.2 сурет – Желілерге қауіп

1.3 Шифрлау және криптография

Зиянды трафикті болдырмауға және блоктауға қосымша, желінің қауіпсіздігі сонымен бірге деректердің қорғалуын талап етеді. Криптография, ақпаратты жасыруды зерттеу және тәжірибе қазіргі заманғы желілік қауіпсіздікте кеңінен қолданылады. Бүгінгі күні желілік өзара әрекеттесудің әр түрінде осы әрекеттестікті болжалды пайдаланушысынан басқа ешкімнен жасыруға арналған сәйкес хаттама немесе технология бар.

Желілік деректерді әр түрлі криптографиялық қосымшалардың көмегімен шифрлауға болады (рұқсат етілмеген пайдаланушылар оқи алмайды). Екі телефонды пайдаланушылар арасындағы әңгіме шифрлануы мүмкін. Компьютердегі файлдарды да шифрлауға болады. Бұл бірнеше мысалдар. Деректер берілетін барлық жерлерде криптографияны қолдануға болады. Шындығында, барлық байланыс шифрланған үрдіс.

Криптография ақпарат қауіпсіздігінің үш құрамдас бөлігі болып табылатын деректердің құпиялығын қамтамасыз етеді: құпиялылық, тұтастық және қол жетімділік. Ақпараттық қауіпсіздік ақпарат пен ақпараттық жүйені санкцияланбаған кіруден, пайдаланудан, жария етуден, бұзудан, өзгертуден немесе жоюдан қорғаумен байланысты. Шифрлау мәтіндік деректерді жасыру арқылы құпиялылықты қамтамасыз етеді (1.3 сурет). Деректердің тұтастығы, б.а. кез-келген жұмыс кезінде деректерді өзгеріссіз сақтауға хэш-механизмдерді қолдану арқылы қол жеткізіледі. Қол жетімділік, яғни деректердің қол жетімділігі желіні жақсарту тетіктері мен резервтік жүйелермен кепілдендірілген.



1.3сурет - Шифрлау арқылы құпиялылық

Қорғау технологияларының эволюциясы:
- 1993, Cisco GRE Tunnels;
- 1996, Site-to-Site IPsec VPNs;
- 1999, SSH;

- 2000, MPLS VPNs;
- 2001, Remote-Access IPsec VPN;
- 2002, Dynamic Multipoint VPN;
- 2005, SSL VPN;
- 2009, Group Encrypted Transport VPN (GET VPN).

1.4 Шабуыл түрлері

Вирустардан, құрттардан және трояндық жылқылардан басқа көптеген желілік шабуылдар бар.

Шабуылды азайту үшін алдымен шабуылдардың әр түрлі түрлерін жіктеу пайдалы. Желілік шабуылдарды санаттарға бөлу арқылы сіз жеке шабуылдардан гөрі, шабуылдардың түрлерін қарастыра аласыз. Желілік шабуылдардың стандартталған жіктемесі жоқ. Бұл курста қолданылатын әдіс шабуылдарды үш негізгі категорияға жіктейді.

Барлау шабуылдары. Барлау шабуылдары жүйелерді, қызметтерді немесе осалдықтарды санкцияланбаған анықтау мен картаға түсіруді қамтиды. Қайта шақыру шабуылдарында Интернетте ақысыз жүктеу үшін кеңінен қол жетімді пакеттік иістер мен порт сканерлері жиі қолданылады. Барлау сіз кіруге болатын үй, мысалы, бос тұрған үй немесе есігі немесе терезесі ашық үй, сіз көмексіз кіре алатын үйге кірген кездегі ақпараттарға ұқсас.

Кіру шабуылдары. Кіру шабуылдары аутентификация қызметтеріндегі, FTP қызметтеріндегі және веб-қызметтердегі белгілі осалдықтарды веб-тіркелгілерге, құпия дерекқорларға және басқа құпия ақпаратқа қол жеткізу үшін пайдаланады. Кіру шабуылы әртүрлі жолдармен жүзеге асырылуы мүмкін. Кіру шабуылы жүйелік құпия сөздерді табу үшін сөздік шабуылын жиі қолданады. Әр түрлі тілдерге арналған арнайы сөздіктер де бар.

DoS шабуылдары. DoS шабуылдары желі немесе Интернет арқылы өте көп сұраныстар жібереді. Бұл шамадан тыс сұраулар мақсатты құрылғы оңтайлы жұмыс істемеуіне әкеледі. Демек, шабуылға ұшыраған құрылғы заңды қол жеткізу және пайдалану үшін қол жетімсіз болады. Эксплуатацияларды немесе олардың комбинацияларын орындау кезінде DoS шабуылдары баяулайды немесе қосымшалар мен процестерді бұзады

1.4.1 Барлау шабуыл түрлері. Барлау ақпарат жинау ретінде де белгілі және көп жағдайда қол жеткізу немесе DoS шабуылына дейін болады. Барлау шабуылында шабуылдаушы әдетте қай IP мекен-жайдың белсенді екенін анықтау үшін мақсатты желіні соғудан бастайды. Содан кейін шабуылдаушы IP-адрестерде қандай қызметтер немесе порттар бар екенін анықтайды. Nmap - портты сканерлеудің ең танымал қосымшасы. Алынған порт ақпаратына сүйене отырып, шабуылдаушы порттардан қосымшаның түрі мен нұсқасын және мақсатты хостта жұмыс істейтін операциялық жүйені анықтауды сұрайды. Көптеген жағдайларда шабуылдаушылар ұсталу ықтималдығы аз болған кезде кейінірек қолдануға болатын осал қызметтерді іздейді.

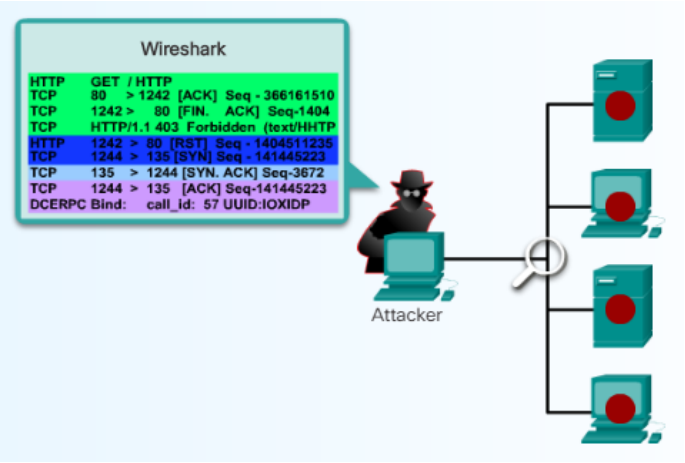
Барлау шабуылдары желіге кіру үшін әртүрлі құралдарды қолданады:

- пакеттік сниферлер;

- пинг-свип;
- портты қарап шығу;
- интернеттен ақпарат сұрату.

Пакет сниффері. Пакеттік сниффер дегеніміз - жергілікті желі арқылы жіберілген барлық желілік пакеттерді ұстап алу үшін желілік адаптер картасын кездейсоқ тәртіпте қолданатын бағдарламалық жасақтама. Тыйым салу режимі - желі адаптерінің картасы өңдеуге өтінім қабылдаған барлық пакеттерді жіберетін режим. Кейбір желілік қосымшалар желілік пакеттерді шифрланбаған таза мәтінмен таратады. Желілік пакеттер шифрланбағандықтан, оларды желіден шығарып, өңдей алатын кез келген қосымша түсінуі мүмкін. 1.4 суретте пакет снифферінің жұмыс істеу мысалы көрсетілген.

Пакеттік сниффер тек шабуылдаушы желімен бірдей қақтығысу доменінде жұмыс істей алады, егер шабуылдаушы аралық қосқыштарға қол жеткізе алмаса. Wireshark сияқты көптеген ақысыз және жалпы пакеттер қол жетімді.



1.4 сурет – Пакет сниффері мысалы

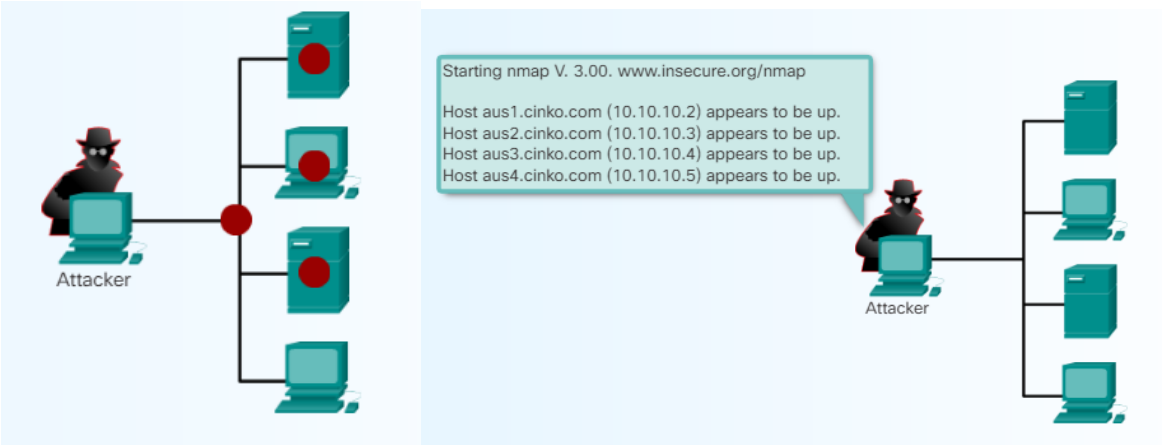
1.4.2 Пинг-свип және портты сканерлеу. Заңды құрал ретінде пайдаланылған кезде, пинг-свип және портты сканерлеу осал қызметтерді анықтау үшін хосттар мен құрылғыларға қарсы бірқатар сынақтар жүргізеді. Ақпарат IP-мекен-жай мен портты немесе баннерді, Трансмиссияны басқару протоколының (TCP) және пайдаланушының деректер схемасы протоколының (UDP) екі портындағы мәліметтерді зерттеу арқылы жиналады. Бұл ақпаратты қаскүнем жүйені бұзу үшін пайдаланады.

Интернеттегі ақпараттық сұраулар белгілі бір доменді кім иеленетіні және осы доменге қандай мекен-жайлар берілгені сияқты ақпаратты ашуы мүмкін. Сондай-ақ, олар нақты IP мекенжайын кім иеленетінін және сол мекенжаймен қай домен байланысты екенін анықтай алады.

Пинг-свип - бұл IP-мекен-жайлардың қайсысы нақты хосттарға сәйкес келетінін анықтайтын желіні сканерлеудің негізгі әдісі. Жалғыз пинг желіде

көрсетілген хосттың бар-жоғын көрсетеді. Пинг сканері бірнеше түйіндерге жіберілген ICMP эхо сұрауларынан тұрады. Егер көрсетілген мекен-жай болса, мекенжай ICMP эхо-жауап қайтарады. Пингті қарап шығу - бұл желіні сканерлеуде қолданылатын ескі және баяу әдістердің бірі. Пинг-свиптің жұмыс істеу мысалы 1.5 суретте көрсетілген.

Хосттағы әрбір қызмет белгілі порт нөмірімен байланысты. Портты қарап шығу - тыңдау қызметтерін анықтау үшін хостта TCP немесе UDP порт нөмірлерін қарап шығу. Ол хосттың әр портына хабарлама жіберуден тұрады. Жіберушінің жауабы осы порттың пайдаланылып жатқандығын көрсетеді. Интернеттегі ақпарат сұранысы арқылы анықталған пин-адресті қарап шығу белгілі бір ортадағы тірі түйіндердің тізімін ұсынуы мүмкін. Мұндай тізімді жасағаннан кейін, портты қарап шығу құралдары барлық белгілі порттар арқылы айналып өтіп, пинг-свип көмегімен табылған хосттарда жұмыс істейтін барлық қызметтердің толық тізімін ұсынады. Осыдан кейін хакерлер белсенді қосымшалардың сипаттамаларын тексере алады, бұл осы қызметті бұзуға ниеті бар хакерге пайдалы ақпарат әкелуі мүмкін.



1.5 сурет - Пинг-свип мысалы

1.4.3 Кіру шабуылдары. Хакерлер желілерге немесе жүйелерге шабуылдарды үш себепке байланысты қолданады: мәліметтер алу, қол жетімділік және қол жетімділік артықшылықтары.

Кіру шабуылдары жүйелік құпия сөздерді табу үшін құпия сөз шабуылдарын жиі қолданады. Парольді шабуыл бірнеше жолмен жүзеге асырылуы мүмкін, соның ішінде қатыгез шабуылдар, трояндықтар, IP-ны бұзу және пакеттік снифтер. Алайда, құпия сөз шабуылдарының көпшілігі қолдан жасалған есептік жазбаны немесе енгізілген сөздікке негізделген парольді бірнеше рет анықтауға бағытталған әрекеттерді қамтитын қатыгез шабуылдар болып табылады.

Қатыгез шабуыл көбінесе желі арқылы жұмыс істейтін және сервер сияқты ортақ ресурсқа кіруге тырысатын бағдарламаны қолдану арқылы жүзеге асырылады. Зиянкестер ресурсқа қол жеткізгеннен кейін, ол бұзылған пайдаланушы тіркелгісімен бірдей қатынасу құқығына ие. Егер бұл есептік

жазбада жеткілікті артықшылықтар болса, зиянкестер бұзылған пайдаланушы есептік жазбасының күйі мен пароліндегі кез-келген өзгерістер туралы алаңдамай, одан әрі кіру үшін қор жасай алады.

Мысалы, пайдаланушы Windows серверінің құпия сөзін алу үшін қатыгез шабуыл жасау үшін L0phtCrack немесе LC5 қосымшасын іске қоса алады. Парольді алғаннан кейін, шабуылдаушы барлық пернелер тіркесімдерінің көшірмелерін қажетті мекен-жайға жіберетін кілттер блогын орната алады. Тағы бір мысалда, мақсатты түрде жіберілген және қабылданған барлық пакеттердің көшірмесін белгіленген бағытқа жіберетін трояндық атты орнатуға болады, ол сізге осы серверге және сол жерден келетін барлық трафикті бақылауға мүмкіндік береді.

Кіру шабуылының бес түрі бар:

- парольмен шабуыл - шабуылдаушы жүйенің құпия сөздерін білуге тырысады. Жалпы мысал - сөздікке шабуыл;

- сенімді пайдалану - шабуылдаушы жүйеге берілген артықшылықтарды санкцияланбаған түрде пайдаланады, бұл мақсаттың бұзылуына әкелуі мүмкін;

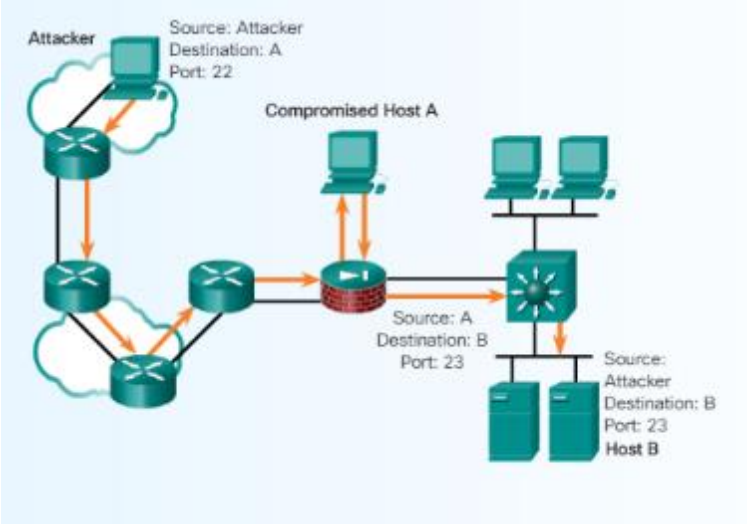
- портты қайта жіберу - бұзылған жүйе басқа нысанаға шабуыл жасау үшін ауысу нүктесі ретінде қолданылады. Басқа нысанаға шабуыл жасау үшін өтпелі нүкте ретінде бұзылған түйінді пайдаланатын сенімді пайдалану түрі. Сеансты қайта бағыттау үшін қол сұғу құралы бұзылған жүйеде орнатылған. Ол мұны басқаша түсіп кетуі мүмкін желілік экран арқылы өткізу үшін жасайды. Шабуыл түрі 1.6 суретте көрсетілген;

- ортаңғы шабуыл - шабуылдаушы екі заңды тұлғаның арасындағы деректерді оқу немесе өзгерту үшін екі заңды тұлға арасындағы байланыстың ортасында. Ортаңғы танымал шабуыл - бұл ноутбукке шабуыл, ол мақсатты қолданушы жіберген барлық желілік трафикті ұстап алып, көшіруге рұқсат етілмеген кіру нүктесі ретінде әрекет етеді. Көбінесе пайдаланушы сымсыз кіру нүктесінде көпшілік алдында болады;

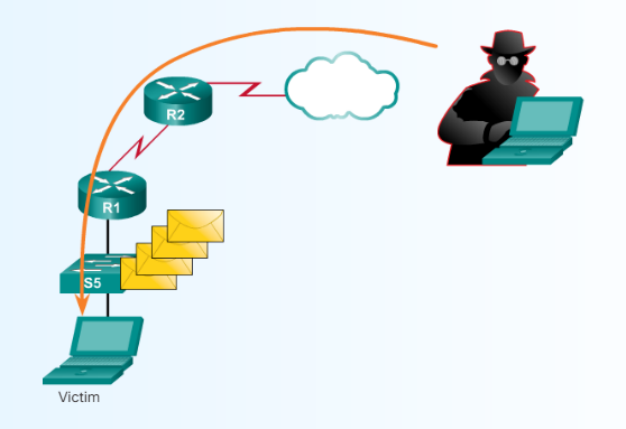
- буфердің толуы - бағдарлама деректерді бөлінген буферлік жадтың сыртына жазады. Буфердің толуы әдетте C немесе C ++ бағдарламасындағы қателікке байланысты болады. Толып кетудің нәтижесі - нақты деректер қайта жазылады немесе зиянды кодты орындау үшін қолданылады. Бұл мысалда шабуылдаушы бағдарламаға қосымша кірістер жіберіп, буфердің толып кетуіне әкеліп соқтырады (1.7 сурет). Толып кетуді бағдарламалық айнымалылардың мәндерін өзгерту үшін және бағдарламаның жоспарланбаған орындарға секіруіне немесе тіпті бағдарламалық кодтың жарамды нұсқаларын еркін кодпен ауыстыруға қолдануға болады.

1.4.4 DoS шабуылдары. DoS шабуылы - бұл пайдаланушыларға, құрылғыларға немесе қосымшаларға қызмет көрсетудің бұзылуына әкелетін желілік шабуыл. DoS шабуылына бірнеше механизм әсер етуі мүмкін. Қарапайым әдіс - бұл нақты желі трафигі болып көрінетін үлкен көлемді шығару. DoS желісіне шабуылдың бұл түрі желіні қанықтырады, осылайша нақты пайдаланушылар трафигін өткізіп жіберуге болмайды.

DoS шабуылы мақсатты жүйелер, мысалы серверлер мәртебе туралы ақпаратты қолдауы керек екенін қолданады. Бағдарламалар күтілетін буферлік өлшемдерге және желілік пакеттердің нақты мазмұнына сене алады.



1.6 сурет - Портты қайта жіберу



1.7 сурет – Буфердің толуы

DoS шабуылы мұның артықшылығын қабылдаушы қолданба күтпеген өлшемдер немесе деректер пакеттері арқылы жібереді.

DoS шабуылының бір мысалы - улы пакет жіберу. Улы пакет - қабылдаушы құрылғыны пакетті дұрыс емес өңдеуге мәжбүрлейтін дұрыс пішімделмеген пакет. Улы пакет қабылдау құрылғысының істен шығуына немесе өте баяу болуына әкеледі. Бұл шабуыл құрылғыдағы барлық байланыстардың бұзылуына және керісінше әкелуі мүмкін. Басқа DoS мысалында шабуылдаушы белгілі бір құрылғыға пакеттердің үздіксіз ағынын жібереді. Бұл соңғы құрылғының қол жетімді ресурстарының шамадан тыс жүктелуіне әкелуі мүмкін, нәтижесінде құрылғы жауап бермейді.

Үлестірілген DoS шабуылы (DDoS) DoS шабуылына ұқсас, тек DDoS шабуылы бірнеше келісілген көздерден болатын жағдайларды қоспағанда.

DDoS шабуылы желілік қауіпсіздік маманынан трафиктің өсуін басқару кезінде таратылған көздерден жасалған шабуылдарды анықтап, тоқтатуды талап етеді.

Мысал ретінде DDoS-нің келесі шабуылы келтірілген:

- хакер қол жетімді жүйелерді қарап шығады;

- хакер бірнеше жүйелерді «өңдеушілерге» қол жеткізгеннен кейін, оларға зомби бағдарламасын орнатады;

- содан кейін зомби агенттерді тексеріп, жұқтырады;

- хакер агенттік жүйелерге қол жеткізген кезде, DDoS шабуылын орындау үшін хакер қашықтан шабуыл бағдарламалық жасақтамасын жүктейді.

DoS шабуылының екі негізгі себебі бар:

- хост немесе бағдарлама күтпеген жағдайларды, мысалы, пішімделген енгізу, жүйелік компоненттердің күтпеген әрекеттестігі немесе қарапайым ресурстардың сарқылуы сияқты жағдайларды жеңе алмайды;

- желі, хост немесе қосымша үлкен көлемде деректерді өңдей алмайды, бұл жүйенің қалыпты жұмысының тоқтатылуына немесе оның баяулауына әкеледі.

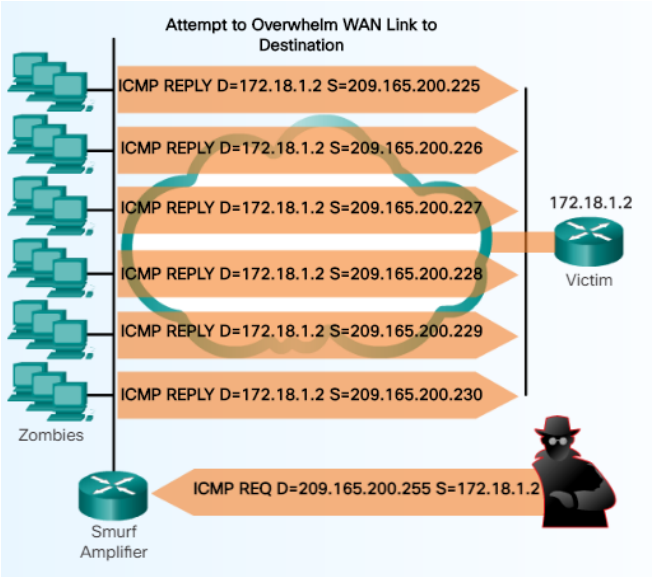
DoS шабуылдары желінің, хосттың немесе бағдарламаның қол жетімділігін бұзуға тырысады. Олар елеулі тәуекел деп саналады, өйткені олар бизнес-процесті оңай тоқтатып, айтарлықтай шығындарға әкелуі мүмкін. Бұл шабуылдарды тіпті тәжірибесіз қаскүнемдер де оңай салыстыра алады.

Кең таралған DoS шабуылына мыналар кіреді:

- Өлім пингі. Өлім шабуылында хакер IP пакетіне жаңғырық сұранысын жібереді, ол 65,535 байттың максималды мөлшерінен асады. Осы өлшемдегі пингтерді жіберу мақсатты компьютерді бұзуы мүмкін. Бұл шабуылдың нұсқасы - нысанаға жиналу буферін толтыратын ICMP фрагменттерін жіберу арқылы жүйені бұзу;

- Smurf шабуылы. Бұл шабуылда, 1.8 суретте көрсетілгендей, шабуылдаушы көптеген ICMP сұрауларын жіберілген адрестерге жібереді, олардың барлығы тиісті желідегі жалған бастапқы мекен-жайлары бар. Егер телерадио хабарларын тарататын мекен-жайларға жеткізетін бағыттаушы құрылғы бағытталған хабарлау сұрауларын қайта бағыттайтын болса, тағайындалған желілердегі барлық түйіндер трафикті желілердегі түйіндердің санына көбейтіп, ICMP жауаптарын жібереді. Мультимедиялық тарату желісінде жүздеген машиналар әр пакетке жауап бере алады;

- TCP SYN Flood шабуылы. TCP SYN су тасқыны TCP SYN пакеттерінің ағынын жиі жалған жіберушінің мекен-жайымен жібереді. Әр пакет қосылу сұранысы ретінде өңделеді, серверді ашық ашық қосылысты бастауға мәжбүр етеді, TCP SYN-ACK пакетін қайтарады және жіберуші мекен-жайы бойынша пакетті күтеді. Алайда, жіберушінің мекен-жайы жалған болғандықтан, жауап ешқашан келмейді. Ашық ашық қосылымдар сервер жасай алатын қосылыстардың санын қанықтырады, бұл шабуыл аяқталғанға дейін заңды сұрауларға жауап бермейді.



1.8 сурет - Смурф шабуылы

DoS шабуылдары үлкен шабуылдың құрамдас бөлігі бола алады. DoS шабуылдары шабуылға ұшыраған компьютерлердің желілік сегменттерінде проблемаларға әкелуі мүмкін. Мысалы, шабуыл нәтижесінде Интернет пен жергілікті желі арасындағы маршрутизатордың өткізу қабілеттілігі артуы мүмкін, бұл тек мақсатты жүйеге ғана емес, бүкіл желіге қауіп төндіреді. Егер шабуыл жеткілікті ауқымда жүргізілсе, Интернет байланысының барлық географиялық аймақтарына қауіп төнуі мүмкін.

Қызметтің барлық өшірулері, тіпті зиянды әрекеттердің салдары да міндетті түрде DoS шабуылдары болып табылмайды. Алайда, DoS шабуылдары ең қауіпті шабуылдардың бірі болып табылады және желілік қауіпсіздік мамандары мұндай шабуылдардың салдарын азайту үшін тез әрекет етуі маңызды.

Дипломдық жобаның мақсаты болып қазіргі заманғы байланыс желілеріне төнетін қауіп түрлерін және онымен күресу әдістерін қарастыру болып табылады

Осы мақсатқа жету үшін келесі міндеттер қойылады:

- қазіргі заманғы желінің қауіпсіздік қатерлерін талдау;
- желіні қорғау әдістерін талдау;
- қондырғыларды негізгі қауіпсіздік шараларымен қамтамасыз ету әдістерін көрсету;
- IPS жүйесінің тиімділігін көрсету.

2 Желіні қорғау әдістері

2.1 Желі шабуылдарын жұмсарту

2.1.1 Барлау шабуылдарын жұмсарту. Мықты аутентификацияны қолдану пакеттік сниферлерінен бірінші қорғаныс болып табылады. Күшті аутентификация - бұл оңай айналып өтуге болмайтын пайдаланушының аутентификациялау әдісі. Бір реттік пароль (OTP) - бұл күшті аутентификация нысаны [4]. OTP екі факторлы аутентификацияны қолданады, ол біреудің қолында бар нәрсені, мысалы, карточканы басқа біреу білетін нәрсемен, мысалы, PIN-кодпен біріктіреді. Банкоматтар екі факторлы аутентификацияны қолданады.

Шифрлау пакеттік сниффер шабуылдарын жеңілдетуде де тиімді. Егер трафик шифрланған болса, онда пакеттік анализаторды пайдалану аз болады, өйткені түсірілген мәліметтер оқылмайды.

Снифтерге қарсы бағдарламалық қамтамасыздандыру және бағдарламалық қамтамасыздандыру хосттардың трафиктік жүктемелерінен гөрі көбірек трафикті өңдейтінін анықтау үшін хост жауап беру уақытының өзгеруін анықтайды. Бұл қауіпті толығымен жоймағанымен, алдын-алудың жалпы жүйесінің бөлігі бола отырып, қауіптің жағдайларын азайтуға мүмкіндік береді.

Ауыстырылған инфрақұрылым қазіргі кездегі норма болып табылады, бұл біздің тікелей соқтығысу доменіміздегі деректерді қоспағанда, кез келген деректерді ұстап қалуды қиындатады, мүмкін бір ғана түйін бар. Ауыстырылған инфрақұрылым пакеттік атқыштардың қаупін жоя алмайды, бірақ шылымшылардың тиімділігін айтарлықтай төмендетеді.

Портты қарап шығуды азайту мүмкін емес, бірақ Интрузияның алдын-алу жүйесін (IPS) және желілік экранды пайдалану портты қарап шығу құралымен анықталатын ақпаратты шектеуі мүмкін. Егер шеткі маршрутизаторларда ICMP жаңғырығын және эхо жауаптары өшірілген болса, пин-қарап шығуды тоқтатуға болады; алайда, бұл қызметтер өшірілгенде, желілік диагностикалық деректер жоғалады. Сонымен қатар, портты сканерлеу толық пингтік тексерусіз орындалуы мүмкін. Сканерлеу жай уақытты алады, өйткені белсенді емес IP мекенжайлар да қарап шығады.

2.1.2 Кіру шабуылдарын жұмсарту. Кіру шабуылдарының таңқаларлық саны парольді немесе сөздік шабуылын болжау арқылы болжау арқылы жасалады. Шифрланған немесе толтырылған түпнұсқалық растама протоколдарын пайдалану, парольді берік саясатпен қатар, сәтті қол жеткізу шабуылдарының ықтималдығын айтарлықтай төмендетеді. Құпия пароль саясатын қамтамасыз ететін арнайы әдістер бар:

- белгілі бір сәтсіз кіруден кейін есептік жазбаларды өшіру. Бұл тәжірибе парольдердің үнемі әрекетіне жол бермейді;
- мәтіндік құпия сөздерді пайдаланбау. Бір реттік парольді немесе шифрланған құпия сөзді пайдаланыңыз;

- күшті парольдерді қолдану.

Күшті парольдер кемінде сегіз таңбадан тұрады және олар үлкен, кіші әріптер, сандар және арнайы таңбалардан тұрады.

Желі ең төменгі сенімділік қағидаты бойынша жасалуы керек. Бұл жүйелер бір-бірін қажетсіз пайдаланбауы керек дегенді білдіреді. Мысалы, егер сіздің ұйымда веб-серверлер сияқты сенімді құрылғылар қолданатын сенімді сервер болса, онда сенімді сервер сөзсіз құрылғыларға сөзсіз сенбеуі керек.

Криптография кез-келген заманауи қауіпсіз желінің маңызды құрамдас бөлігі болып табылады. Желіге қашықтан кіру үшін шифрлауды пайдалану ұсынылады. Маршруттау хаттамасының трафигі де шифрланған болуы керек. Неғұрлым трафик шифрланған болса, хакерлердің «ортасында шабуылшы» сияқты шабуылдарды қолдана отырып, деректерді ұстап алу мүмкіндігі азаяды.

2.1.3 DoS шабуылдарын жұмсарту**.** Интернетте қатысу деңгейі жоғары компаниялар ықтимал жұмсарту әдістерін ұсына отырып, ықтимал DoS шабуылдарына қалай әрекет етуді алдын-ала жоспарлауы керек. Тарихқа сәйкес, көптеген DoS шабуылдары жалған бастапқы мекен-жайлардан туындаған [5]. Периметрлік маршрутизаторлар мен желілік экрандарда антифафакциялық технологиялар көмегімен мұндай шабуылдарды болдырмауға болады. Бүгінгі күні көптеген DoS шабуылдары бірнеше желілерде бұзылған түйіндер жасаған DoS шабуылдары. DDoS шабуылдарының салдарын азайту үшін мұқият диагностика, жоспарлау және провайдерлердің бірлескен жұмысы қажет. DoS шабуылдарын азайтудың маңызды элементтері брандмауэр және IPS болып табылады. 2.1 суретте Cisco IPS 4200 Series Sensors қондырғысы көрсетілген.

Cisco маршрутизаторлары мен коммутаторлары әртүрлі қорғаныс технологияларын қолдайды, мысалы, портты қорғау, хосттың динамикалық конфигурация протоколы (DHCP), IP көзін қорғау, мекен-жайдың динамикалық протоколы (ARP) және қол жеткізуді басқару тізімдері (ACLs). .

Сонымен, қызмет көрсету сапасы (QoS) қауіпсіздік технологиясы болмаса да, оның қолданылуының бірі - трафик қауіпсіздігі - кез-келген клиенттен келетін трафикті шектеу үшін пайдаланылады. Бұл бір көздің өткізу қабілетін пайдалануға әсерін шектейді.

2.1 сурет - Cisco IPS 4200 Series Sensors

2.1.4 Желіні қорғау. Желіні шабуылдан қорғау үнемі қырағылық пен білімді қажет етеді. Төменде желіні қорғаудың ең жақсы тәжірибелері келтірілген:

Мүмкіндігінше буфердің толып кетуіне және артықшылықтардың өршуіне жол бермеу үшін, оларды апта сайын немесе күн сайын орнатып, түзетулерді жаңарту керек:

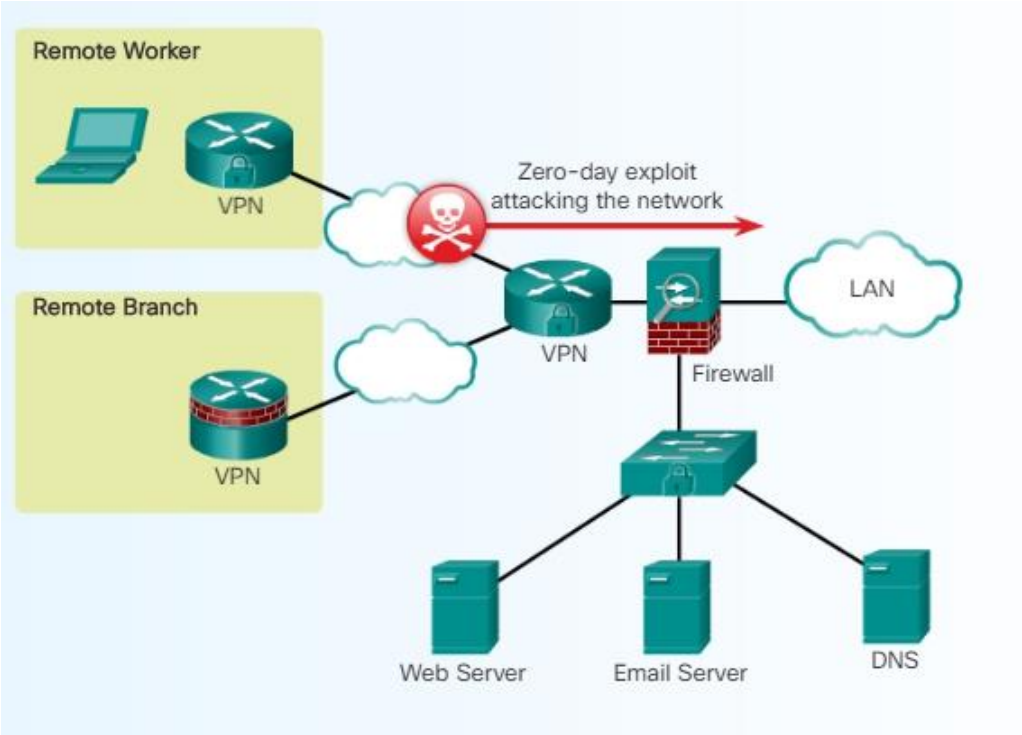
- қажетсіз қызметтер мен порттарды өшіру;
- күшті парольдерді пайдалану және оларды жиі өзгертіп тұру;
- жүйелерге физикалық қол жетімділікті басқару;
- веб-парақтың қажетсіз кірістерінен аулақ болу.
- кейбір веб-сайттар пайдаланушыларға пайдаланушы аттары мен парольдерді енгізуге мүмкіндік береді. Хакер тек қолданушы атымен ғана кіре алмайды. Мысалы, «jdoe; rm -rf /» енгізу зиянкестерге файлдық жүйені UNIX серверінен жоя алады. Бағдарламалаушылар енгізу таңбаларын шектеуі керек және | сияқты жарамсыз таңбаларды қабылдамауы керек; <> енгізу ретінде;;
- сақтық көшірме жасау және сақтық көшірме жасалған файлдарды үнемі тексеріп отыру;
- қызметкерлерді әлеуметтік инженерлік қауіп-қатерлер туралы хабардар ету және жеке басын сәйкестендіруді телефон арқылы, электрондық пошта арқылы немесе жеке тұлға арқылы растау стратегиясын жасау;
- шифрлау және құпия сөзбен қорғалған құпия мәліметтер;
- желілік экран, IPS, виртуалды жеке желі (VPN) құрылғылары, антивирустық бағдарламалық қамтамасыз ету және мазмұнды сүзу сияқты қауіпсіздік техникасы мен бағдарламалық жасақтамасын іске қосу;
- компания үшін жазбаша қауіпсіздік саясатын әзірлеу.

Бұл әдістер қауіпсіздікті басқарудың бастапқы нүктесі ғана. Ұйымдар үнемі дамып келе жатқан қауіп-қатерлерден қорғану үшін әрдайым қырағы болуы керек.

2.2 IPS жүйесі

2.2.1 Zero-day шабуылдары. Интернеттегі құрттар мен вирустар бірнеше минут ішінде бүкіл әлемге тарала алады. Желі құрт пен вирустың қауіптерін бірден біліп, азайтуға тиіс. Желілік экрандар көп нәрсені жасай алады және зиянды бағдарламалар мен нөлдік шабуылдардан қорғай алмайды [6].

Zero-day, кейде нөлдік күндік қауіп деп аталады, бағдарламалық жасақтама жеткізушісі белгісіз немесе жарияламайтын осалдықтарды пайдалануға тырысатын компьютерлік шабуыл (2.2 сурет). Нөлдік сағат термині эксплуатацияның ашылған сәтін сипаттайды. Уақыт өте келе бағдарламалық жасақтаманы сатушыға патчты әзірлеу және шығару қажет болады, желі бұл эксплуатацияға осал болады. Осы жылдам қозғалатын шабуылдардан қорғану үшін желілік қауіпсіздік мамандарынан желілік архитектураның жетілдірілген көрінісі қажет. Желідегі бірнеше нүктеде интрузияны қамту мүмкін емес



2.2 сурет - Zero-Day Exploit шабуылы

2.2.2 Шабуылдарды бақылау. Желіге құрттар мен вирустардың енуіне жол бермеудің бір тәсілі - әкімшіні желіні үнемі бақылап отыру және желілік құрылғыларда пайда болған журнал файлдарын талдау. Бұл шешім өте ауқымды емес. Журнал файлдарындағы ақпараттарды қолмен талдау көп уақытты талап етеді және желіге шабуылдар туралы шектеулі түсінік алуға мүмкіндік береді. Бөренелер талданған кезде шабуыл басталып кетті.

Желідегі трафикті пассивті бақылау үшін IDS енгізілді. IDS бар құрылғы трафик ағынын көшіретінін және жіберілген пакеттерді емес, көшірілген трафикті талдайтынын көрсетеді. Офлайн режимінде жұмыс істеген кезде, ол траффиктің ағынын белгілі зиянды қолдармен, вирустарды тексеретін бағдарламалық жасақтамамен салыстырады. Дербес күйде жұмыс істеу IDS енжар екенін білдіреді; IDS құрылғысы желіде нақты орналасқан, сондықтан оған жету үшін трафикті көрсету керек; егер ол көрсетілмесе, желі трафигі IDS арқылы өтпейді. Трафик бақыланады және хабарлануы мүмкін, бірақ IDS тікелей пакеттерге ешқандай әрекет жасамайды. IDS-тің бұл дербес іске асырылуы «режим» деп аталады.

Көшірме трафигімен жұмыс істеудің артықшылығы - IDS жіберілген трафиктің нақты пакеттік ағымына теріс әсер етпейді. Көшірме трафигімен жұмыс істеудің кемшілігі - IDS шабуылға жауап бермес бұрын зиянды шабуылдарды бір пакетпен тоқтата алмайтындығында. IDS шабуылына жауап беру көбінесе маршрутизаторлар мен брандмауэр сияқты басқа желілік құрылғылардың көмегін қажет етеді.

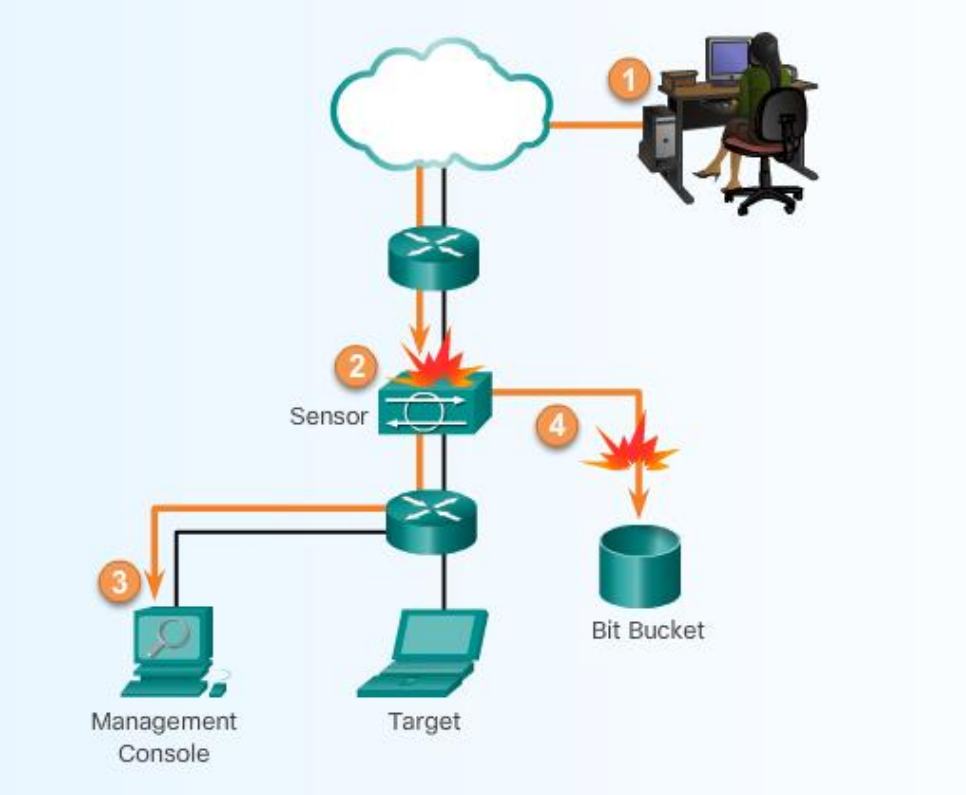
Жақсы шешім - шабуылды дереу анықтап, тоқтата алатын құрылғыны пайдалану. IPS бұл функцияны орындайды.

2.2.3 Шабуылдарды анықтау және тоқтату. IPS IDS технологиясына негізделген. IDS-тен айырмашылығы, IPS құрылғысы ендіру режимінде жүзеге асырылады. Бұл барлық кіріс және шығыс трафик өңделуі үшін ол арқылы өтуі керек дегенді білдіреді. IPS пакеттерге алдын-ала талдаусыз желінің сенімді жағына кіруге мүмкіндік бермейді. Ол желі мәселесін анықтап, дереу шеше алады.

IPS 3 және 4 деңгейдегі трафикті бақылайды және 2-7 деңгейдегі зиянды деректерді қамтуы мүмкін күрделі шабуылдар үшін пакеттердің мазмұны мен жүктемесіне талдау жасайды. Cisco IPS платформалары анықтаушы технологиялардың, соның ішінде сигнатураны анықтауды, профильді және протоколды талдауды қолданады. Бұл терең талдау IPS-ге әдеттегі брандмауэр құрылғысынан өтетін шабуылдарды анықтауға, тоқтатуға және блоктауға мүмкіндік береді. Пакет IPS интерфейсі арқылы келген кезде, пакет талданғанша шығыс немесе сенімді интерфейске жіберілмейді.

Тізбектелген режимде жұмыс істеудің артықшылығы - IPS бір пакеттік шабуылды мақсатты жүйеге жетуіне жол бермейді. Кемшілігі - нашар теңшелген IPS немесе пропорционалды IPS шешімі жіберілген трафиктің пакеттік ағымына кері әсер етуі мүмкін.

IDS және IPS арасындағы ең үлкен айырмашылық - бұл IPS дереу жауап береді және зиянды трафикке жол бермейді, ал IDS зиянды трафиктің қарастырылуына дейін өтуіне мүмкіндік береді (2.3 сурет).



2.3 сурет - IDS операциясы

2.2.4 IDS және IPS артықшылықтары мен кемшіліктері**.** IDS платформасының басты артықшылықтарының бірі - оны офлайн режимде орналастыру. IDS сенсоры желіге қосылмағандықтан, бұл желі жұмысына әсер етпейді. Ол кідіріс, діріл немесе басқа трафик ақауларын тудырмайды. Сонымен қатар, егер сенсор сәтсіз болса, бұл желінің жұмысына әсер етпейді. Бұл тек IDS деректерді талдау қабілетіне әсер етеді.

Алайда, IDS платформасын орналастырудың көптеген кемшіліктері бар. IDS сенсоры ең алдымен ықтимал инциденттерді анықтауға, олар туралы ақпаратты жазуға және осы әрекеттер туралы есеп беруге бағытталған. IDS сенсоры іске қосу пакетін тоқтата алмайды және байланыстың тоқтауына кепілдік бермейді. Олар сонымен қатар пошта вирусын және құрттар сияқты автоматтандырылған шабуылдарды тоқтату үшін азырақ пайдалы емес.

IDS сенсорының әрекет ету әрекеттерін қолданатын пайдаланушыларда IDS қолдану процесін жақсы түсінумен үйлескен қауіпсіздік саясаты болуы керек. Пайдаланушылар кіруді анықтаудың күтілетін деңгейіне жету үшін IDS сенсорларын орнатуға уақыт жұмсауы керек.

Ақырында, IDS сенсорлары желіге біріктірілмегендіктен, IDS енгізу желінің шабуылының әртүрлі әдістеріне қосылған желілік қауіпсіздіктен жалтару әдістеріне осал болып келеді.

2.2.5 IPS артықшылықтары мен кемшіліктері**.** IPS платформасын сериялық режимде қолдану оның артықшылықтары мен кемшіліктеріне ие.

IDS-тің бір артықшылығы - IPS сенсоры триггер пакетін, қосылуға байланысты пакеттерді немесе бастапқы IP адресінен пакеттерді тоқтату үшін пакетті тастауға конфигурациялануы мүмкін. Сонымен қатар, енгізілген кезде, IPS ағындарды қалыпқа келтіру әдістерін қолдана отырып, желінің қауіпсіздігінен жалтаруға мүмкіндік береді.

IPS-тің кемшілігі - қателіктер, сәтсіздіктер және тым көп трафикпен IPS сенсорының шамадан тыс жүктелуі желінің жұмысына теріс әсер етуі мүмкін. Себебі, IPS желіде орналасуы керек және трафик одан өтуі керек. IPS кідірістер мен дірілдерді енгізу арқылы желінің жұмысына әсер етуі мүмкін. IPS VoIP сияқты уақытқа тәуелді қосымшаларға теріс әсер етпеуі үшін тиісті түрде өлшеніп, енгізілуі керек.

Орналастыруды қарастыру. Осы технологиялардың біреуін қолдану екіншісін пайдаланудан бас тартпайды. Шындығында, IDS және IPS технологиялары бір-бірін толықтыра алады. Мысалы, IDS IPS жұмысын тексеру үшін енгізілуі мүмкін, өйткені IDS пакеттік тексеруді дербес режимде жүргізуге теңшелуі мүмкін. Бұл IPS-ке азырақ, бірақ аса маңызды, нақты уақыттағы трафиктің құрылымына назар аударуға мүмкіндік береді.

Пайдалану туралы шешім желінің қауіпсіздік саясатында көрсетілгендей ұйымның қауіпсіздік мақсаттарына негізделеді.

2.2.6 Желілік IPS сенсорлар. Желілік IPS IPS 4200 сериялары сияқты арнайы IPS құрылғысын қолдану арқылы жүзеге асырылуы мүмкін. Сонымен қатар, оны ISR, ASA брандмауэріне немесе Catalyst 6500 коммутаторына қосуға болады IPS желілік шешімдері интрузияның алдын-алудың маңызды

құрамдас бөлігі болып табылады.

2.1 кесте - IDS және IPS салыстыру

	Артықшылықтары	Кемшіліктері
IDS	-желіге әсер етпейді (кідіріс, діріл) - Желіге әсер етпейді, егер болса сенсордың ақаулығы - Желіге әсер етпейді, егер болса сенсордың шамадан тыс жүктелуі	- жауап әрекеттері триггер пакеттерін ұстай алмайды - жауап әрекеті үшін қажетті дұрыс баптау - жауапкершіліктен жалтарудың желілік әдістеріне көбірек осал
IPS	- Триггерлік пакеттерді тоқтатады - Қалыпқа келтіру әдістер ағынын қолдануға болады	- Датчиктермен проблемалар желілік трафикке әсер етуі мүмкін - сенсорлық жүктеме желісінің әсері - желіге әсер ету (кідіріс, діріл)

Хостқа негізделген IDS / IPS шешімдері бар болғанымен, қауіпсіздіктің се-німді архитектурасын қамтамасыз ету үшін оларды IPS желілік шешімдерімен біріктіру қажет.

Сенсорлер зиянды және рұқсат етілмеген әрекеттерді нақты уақытта анықтайды және қажет болған жағдайда шаралар қолдана алады. Сенсорлар белгілі бір желілік нүктелерде орнатылады, бұл қауіпсіздік менеджерлеріне шабуылдың қай жерде болғанына қарамастан, оның желілік әрекетін бақылауға мүмкіндік береді.

Сенсорларды бірнеше жолмен іске асыруға болады:

- жетілдірілген біріктірілген модуль (AIM-IPS) немесе жетілдірілген желілік модуль (NME-IPS) бар немесе жоқ ISR-де;

- қауіпсіздікті және алдын-алудың кеңейтілген модулі бар немесе онсыз ASA брандмауэр құрылғысында (ASA AIP-SSM);

- интрузияны анықтау модулі (IDSM-2) көмегімен Catalyst 6500 қосылды;

- Cisco IPS 4200 сериялы сенсор сияқты жеке құрылғы ретінде.

IPS желілік сенсорлары әдетте кедергі келтірудің алдын-алу талдауы үшін конфигурацияланған. IPS модулі орнатылған платформаның негізгі операциялық жүйесі қажетсіз желілік қызметтерден айырылған және негізгі қызметтер қорғалған. Мұны сөндіру деп атайды. Жабдық үш компоненттен тұрады:

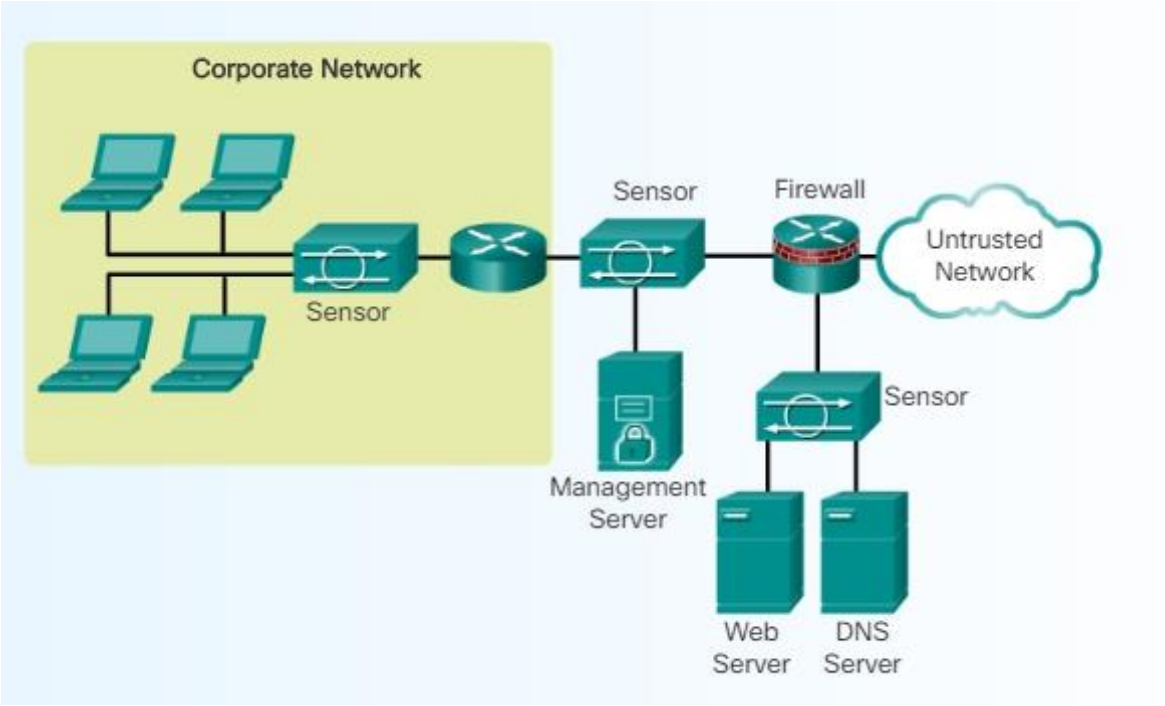
- NIC - Желілік IPS Ethernet, Fast Ethernet және Gigabit Ethernet сияқты кез келген желіге қосыла алуы керек;

- процессор - интрузияның алдын-алу процедураның енуін анықтауды және үлгіні сәйкестендіру үшін процессордың күшін қажет етеді;

- жад - басып кіруді анықтау үшін көп жад қажет. Жад IPS желісінің шабуылды тиімді және дәл анықтай алу қабілетіне тікелей әсер етеді.

Желілік IPS қауіпсіздік менеджерлеріне, өсуіне қарамастан, нақты

уақыттағы желінің қауіпсіздігі туралы ақпараттар береді. Қосымша сенсорларды қажет етпестен қауіпсіз желілерге қосымша хосттарды қосуға болады. Қосымша сенсорлар олардың өткізу қабілеттілігі жоғарылаған кезде, олардың өнімділігі қазіргі қажеттіліктерге сәйкес келмеген кезде немесе қауіпсіздік саясатын қарастырғанда немесе желіні жобалағанда қауіпсіздік шекараларын нығайтуға көмектесетін қосымша сенсорларды қажет еткен кезде ғана қажет. Жаңа желілерді қосқан кезде қосымша сенсорлар оңай орналастырылады. 2.4 суретте IPS сенсорларын орналастырудың мысалы көрсетілген.



2.4 сурет -IPS сенсорды орналастыру мысалы

2.2.7 Cisco IPS шешімдері. Cisco 1900, 2900 және 3900 ISR G2 құрылғыларын Cisco немесе IOS қауіпсіздік технологиялары пакетінің құрамдас бөлігі болып табылатын Cisco IOS IPS көмегімен IPS мүмкіндіктерін қолдау үшін CLI немесе Cisco Configuration Professional көмегімен конфигурациялауға болады. Бұл IPS модулін орнатуды қажет етпейді, бірақ сигнатураларды жүктеу үшін сигнатура файлдары мен жадты жүктеуді талап етеді. Дегенмен, мұндай қондырғы шектеулі трафигі бар шағын ұйыммен шектелуі керек.

Трафиктің үлкен көлемінде Cisco IPS сенсорларын оқшауланған құрылғыларды қолдана отырып немесе желілік құрылғыларға қосылған модульдер ретінде қолдануға болады.

Cisco IOS IPS-тен басқа, Cisco модульдік және құрылғыға негізделген IPS шешімдерін ұсынады:

- Cisco IPS жетілдірілген интеграция модулі (AIM) және жетілдірілген желілік модуль (IPS NME) - IPS-ті Cisco ISR-ке біріктіреді және жетілдірілген

IPS мүмкіндіктерін қамтамасыз ету үшін шағын және орта бизнесте (SMB) және филиалдық ортада қолданылады. Cisco 1841, 2800 сериялары және 3800 сериялы ISR-де қолдау көрсетіледі. NME IPS ISR 2800, 3800, 2900 және 3900 серияларында қолданылады;

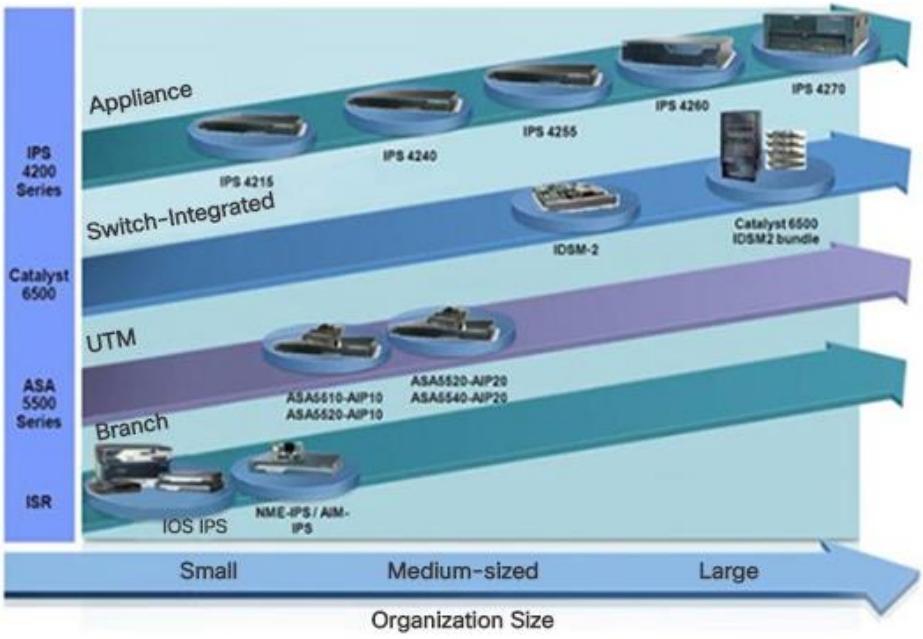
- Cisco IPS жетілдірілген инспекциясы және алдын-алу бойынша қауіпсіздік қызметі модулі (AIP SSM) және қауіпсіздік қызметтерінің картасы (AIP SSC) - Cisco ASA 5500 сериялы бейімделгіш қауіпсіздік техникасы үшін IPS мүмкіндіктерін кеңейтеді 2-суретте AIP SSM-10 үшін Cisco ASA 5510 және 5520 модельдері AIP SSC-5 арнайы Cisco ASA 5505 үшін жасалған.

IPS шешімін таңдау. Сенсорды таңдау ұйымның талаптарына байланысты. IPS сенсорын таңдауға және орнатуға әсер ететін бірнеше факторлар бар:

- желілік трафиктің мөлшері;
- желілік топология;
- қауіпсіздік бюджеті;
- IPS басқару үшін қол жетімді қауіпсіздік персоналы.

2.5 суретте көрсетілгендей, филиалдар сияқты кішігірім бағдарламалар үшін тек Cisco IOS IPS қосылған ISR маршрутизаторы қажет болуы мүмкін. Трафик өскен сайын ISR-ді IPS функцияларын жүктеу үшін конфигурациялауға болады, ол IPS Network Enhanced (NME) немесе IPS Advanced Integration Module (AIM) көмегімен жүзеге асырылады.

Кәсіпорындар мен провайдерлерден IDSM-2 желілік модулін қолдану арқылы арнайы IPS құрылғысы немесе Catalyst 6500 қажет болуы мүмкін.



.

2.5 сурет - IPS шешімін таңдау

2.3 IPS сигнатуралары

2.3.1 Сигнатура төлсипаттары**.** Кіретін зиянды трафикті тоқтату үшін желі алдымен оны анықтай алуы керек. Бақытымызға орай, зиянды трафиктің белгілі бір сипаттамалары немесе сигнатуралары бар [7]. Сигнатура - бұл IDS және IPS DoS шабуылдары сияқты әдеттегі шабуылды анықтау үшін пайдаланатын ережелер жиынтығы. Бұл сигнатураларда белгілі бір құрттар, вирустар, протокол аномалиялары немесе зиянды трафик бірегей болады. IPS сенсорлары тиісті қолдарды немесе трафиктің қалыптарын іздеуге конфигурацияланған. IPS сигнатуралары вирус сканерлері қолданатын virus.dat файлына тұжырымдамалық жағынан ұқсас.

Сенсорлар желілік пакеттерді сканерлейтіндіктен, олар белгілі шабуылдарды анықтау және алдын-ала жасалған әрекеттерге жауап беру үшін сигнатураларды пайдаланады. Зиянды пакеттердің ағымы белгілі бір әрекет түріне және сигнатураға ие. IDS немесе IPS сенсоры көптеген түрлі сигнатуралардың көмегімен мәліметтер ағынын тексереді. Сенсор деректер ағынымен сигнатураға сәйкес келгенде, журналға оқиға жазу немесе IDS немесе IPS басқару бағдарламалық жасақтамасына дабылды жіберу сияқты әрекеттер жасалады.

Сигнатураның үш ерекшелігі бар:

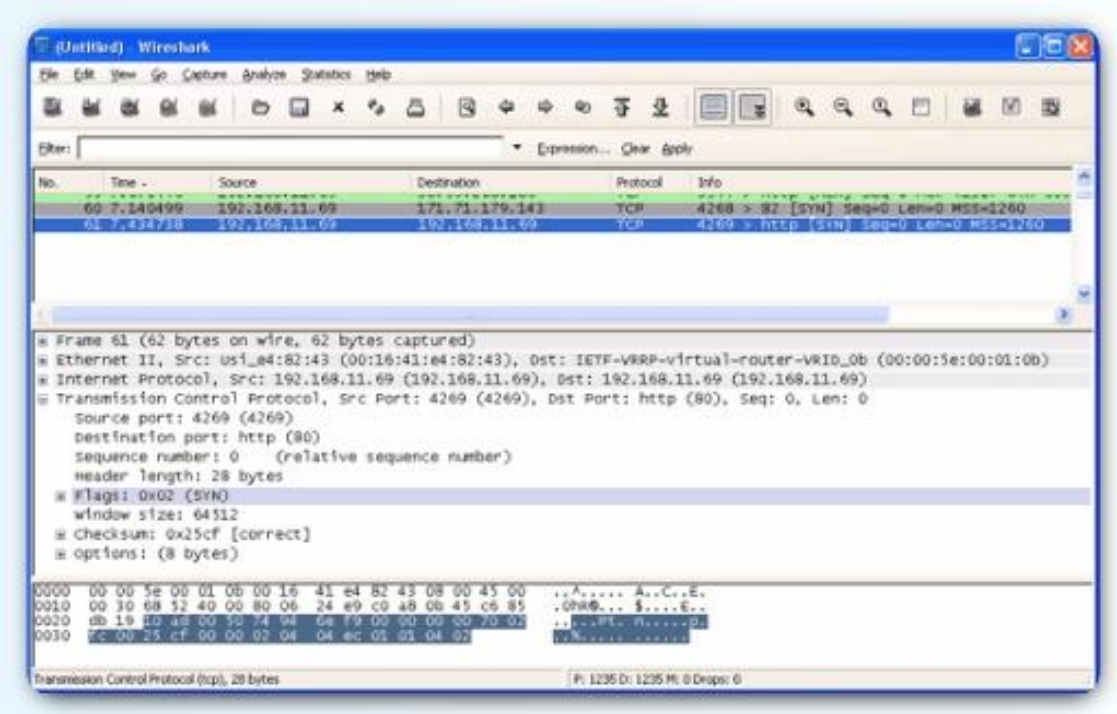
- Types;
- Trigger (дабыл);
- Action.

2.3.2 Сигнатура түрлері. Сигнатура түрлері, әдетте, атомдық немесе қосылыс деп жіктеледі.

Атомдық сигнатура - сигнатураның қарапайым түрі. Ол конфигурацияланған сигнатураның сәйкестігі тексерілетін бір пакеттен, әрекеттен немесе оқиғадан тұрады. Бұл жағдайда дабыл қосылып, сигнатурамен байланысты әрекет орындалады. Бұл сигнатураларды бір оқиғаға сәйкестендіруге болатындықтан, олар күй туралы ақпаратты сақтау үшін қол сұғу жүйесін қажет етпейді. Шарт дегеніміз бір уақытта қосымша түрде алынатын бірнеше ақпарат пакеті талап етілетін жағдайларға жатады. Мысалы, күйді сақтау талабы туындаған жағдайда, IDS немесе IPS орнатылған TCP қосылыстарының үш жақты байланысын бақылауы керек еді. Атомдық сигнатуралар болған жағдайда, барлық тексеру атом операциясы кезінде жүргізілуі мүмкін, ол өткен немесе болашақ әрекеттер туралы білуді қажет етпейді.

Атомдық сигнатураны анықтау IPS немесе IDS құрылғысындағы жад сияқты ең аз ресурстарды қажет етеді. Бұл сигнатураларды анықтау және түсіну оңай, өйткені олар белгілі бір оқиға немесе пакетпен салыстырылады. Осы атомдық қолдардың трафигін талдау әдетте өте тез және тиімді орындалуы мүмкін. Мысалы, LAND шабуылында атомдық сигнатура бар, себебі ол жалған TCP SYN пакетін (қосылысты бастайды) мақсатты хосттың IP-адресімен және мақсатты құрылғыдағы ашық портпен бірдей көзі мен

мақсатты портымен бірдей етіп жібереді. 2.6 суретте. LAND шабуылының себебі - бұл машинаны үнемі өзіне жауап беруге мәжбүр етеді. Шабуылдың бұл түрін анықтау үшін бір пакет қажет. IDS әсіресе атом шабуылына осал келеді, өйткені шабуыл тапқанға дейін зиянды жеке пакеттер желіге жіберіледі. Алайда, IPS бұл пакеттердің желіге мүлдем жетуіне жол бермейді.



2.6 сурет - Қарапайым LAND шабуылын басып алу

Композициялық сигнатура. Композиттік сигнатура мемлекеттік сигнатура деп те аталады. сигнатураның бұл түрі бірнеше хосттар арасында еркін уақыт аралығында таратылған әрекеттер тізбегін анықтайды. Атомдық сигнатуралардан айырмашылығы, құрамды қолдардың мемлекеттік қасиеттері шабуыл сигнатурасымен сәйкестендіру үшін әдетте бірнеше мәліметтер жиынтығын талап етеді, ал IPS құрылғысы күйін сақтауы керек. сигнатуралардың күйін сақтау керек уақыт ұзақтығы оқиға көкжиегі ретінде белгілі.

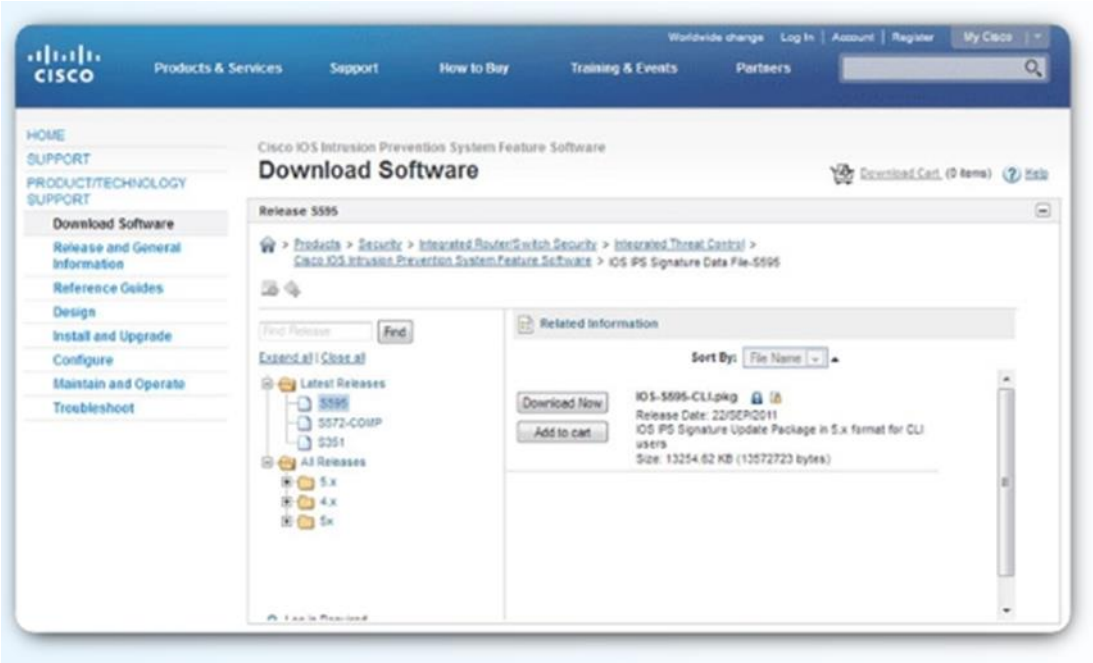
Оқиға көкжиегінің ұзындығы бір сигнатурадан екіншіге дейін өзгереді. IPS мемлекеттік ақпараттарды шексіз мерзімде ресурстардың таусылмай тұра алмайды. Сондықтан IPS бастапқы қол қою компоненті табылған кезде нақты шабуылға сигнатураны қанша уақытқа созылатындығын анықтау үшін конфигурацияланған оқиғалар көкжиегін пайдаланады. Оқиғаның көкжиегін баптау - бұл жүйелік ресурстарды тұтыну мен ұзақ уақыт аралығында болатын шабуылды анықтауға мүмкіндік беретін сауда.

2.3.3 Сигнатура файлы. Желілік қауіпсіздікке төнетін қатер жиі пайда болып, тез таралады. Жаңа қауіптер анықталған сайын жаңа қолдар жасалып, ХТЖ-ға жүктелуі керек. Бұл процесті жеңілдету үшін барлық сигнатуралар сигнатура файлында болады және тұрақты түрде IPS-ке жүктеледі.

Сигнатура файлында IPS немесе IDS функциялары бар Cisco өніндегі резиденттің сигнатурасы туралы мәліметтер базасын жаңарту үшін арналған желілік сигнатуралар пакеті бар. Бұл сигнатура дерекқорын IPS немесе IDS шешімі желілік трафикті сигнатура-файлдар кітапханасындағы деректер үлгісімен салыстыру үшін қолданады. IPS немесе IDS желідегі трафиктің күдікті әрекеттерін анықтау үшін осы салыстыруды пайдаланады.

Мысалы, LAND шабуылы «Мүмкін емес IP пакет» сигнатурасында анықталған (қол 1102.0). сигнатура файлында бұл сигнатура және тағы басқалар бар. Соңғы сигнатура файлдарын қолданатын желілер желілік шабуылдардан жақсы қорғалған. 2.7 суретте Cisco.com-дан қол қойылған сигнатура файлы көрсетілген.

ViscoSign SSL сертификаттарын құрылғыға орнатқаннан кейін Cisco.com-дан алынған IPS сигнатураларын автоматты түрде мерзімді түрде шығаруды ISR G2 құрылғысында конфигурациялауға болады.



2.7 сурет - CCO сигнатура файлдары

2.3.4 Сигнатура микро қозғалтқыштары. Сигнатураны сканерлеуді тиімдірек ету үшін, Cisco IOS бағдарламалық жасақтамасы жалпы сигнатураларды топтарға жіктейтін Micro Signature Motor (SMEs) машиналарына сүйенеді. Cisco IOS бағдарламалық жасақтамасы бір уақытта бір сигнатураны емес, топтық сипаттамаларға негізделген бірнеше сигнатураны сканерлейді.

IDS немесе IPS қосылған кезде, SME маршрутизаторға қосылады немесе орнатылады. SME құрылған кезде маршрутизатор сигнатурада кездесетін тұрақты өрнекті құрастыруды қажет етуі мүмкін. Тұрақты өрнек дегеніміз - байттар қатарында өрнек іздеуді көрсетудің жүйелі әдісі.

Содан кейін SME белгілі бір хаттамадан зиянды әрекеттерді іздейді. Әр

механизм тетік тексеретін протоколдар мен өрістер үшін жарамды диапазондар немесе мәндер жиынтығы бар құқықтық параметрлер жиынтығын анықтайды. Атомдық және құрама пакеттер пакет құрамындағы хаттамаларды танитын микрофон арқылы сканерленеді. Сигнатураны SME ұсынатын параметрлер арқылы анықтауға болады.

Әр SME пакеттен құндылықтарды шығарады және пакеттің бөліктерін қарапайым өрнек қозғалтқышына өткізеді. Regex қозғалтқышы бірден бірнеше үлгіні іздей алады.

Қол жетімді SME платформаға, Cisco IOS нұсқасына және сигнатура файлының нұсқасына қарай әр түрлі болады. Cisco IOS бес микро қозғалтқышты анықтайды:

- атом - ICMP және UDP сияқты қарапайым пакеттерді тексеретін сигнатуралар;
- сервис - көптеген шабуылға ұшыраған қызметтерді тексеретін сигнатуралар;
- String - интрузияны анықтау үшін тұрақты өрнек үлгілерін қолданатын сигнатуралар;
- Multi-string - Trend Labs үлгілері мен сигнатураларының икемді сәйкестігін қолдайды;
- басқа - әртүрлі сигнатураларды өңдейтін ішкі қозғалтқыш.

SME үнемі жаңарып отырады. Мысалы, 12.4 (11) T нұсқасына дейін Cisco IPS сигнатурасының форматы 4.x нұсқасын қолданды. IOS 12.4 (11) T кейін, Cisco 5.x нұсқасын, жетілдірілген IPS сигнатурасы пішімін ұсынды. Жаңа нұсқа шифрланған сигнатура параметрлерін және сигнатура қаупін бағалау сияқты басқа функцияларды қолдайды, мысалы, сигнатураны қауіпсіздік қатері тұрғысынан бағалайды.

Маршрутизатордың сигнатураны қолдауға қойылатын талаптарын анықтау кезінде ескеру қажет бірнеше факторлар бар. Біріншіден, тұрақты өрнекті құрастыру қарапайым өрнекті сақтаудан гөрі көп жадыны қажет етеді. Сигнатураларды жүктеу және біріктіру алдында дайын сигнатураға арналған жадтың соңғы талаптарын анықтау керек. Маршрутизатордың әртүрлі платформалары нақты қанша сигнатура болатынын есептеу. сигнатуралар мен қозғалтқыштардың саны сигнатура бар жадқа байланысты. Осы себепті, ең көп жады бар Cisco IOS IPS қолдайтын маршрутизаторларды іске қосу керек.

2.3.5 Сигнал дабылы**.** Кез-келген IPS сигнатураның негізі - сигнатура сигналы, көбінесе сигнатура триггері деп аталады. Үйдегі қауіпсіздік жүйесін қарастырыру керек. Дабылды күзететін бөлмеге кірген адамның қозғалысын анықтайтын қозғалыс детекторы болуы мүмкін.

IPS үшін сигнатура триггері шабуыл немесе қауіпсіздік саясатын бұзу туралы сенімді түрде кез келген нәрсе болуы мүмкін. Желілік IPS сигнатура әрекетін бастай алады, егер ол белгілі бір портқа баратын белгілі бір жол бар жүктеме пакетін анықтаса. Хостқа негізделген IPS белгілі бір функция шақырылған кезде сигнатура әрекетін тудыруы мүмкін (функционалды қоңырау - басқару және функция дәлелдерін беретін өрнек). Қауіпсіздік

саясатын бұзу немесе бұзу туралы сенімді түрде сигнал бере алатын кез келген нәрсені іске қосу тетігі ретінде пайдалануға болады.

Cisco IPS 4300 сериялары және Cisco Catalyst 6500 IDSM-2 сияқты Cisco IDS және IPS сенсорлары сигнатура триггерлерінің төрт түрін, сонымен қатар олардың артықшылықтары мен кемшіліктерін пайдалана алады:

- Pattern-based анықтау;
- Anomaly based анықтау;
- Policy-based анықтау;
- Honey pot-based анықтау.

Бұл триггер механизмдерін атомдық және құрама сигнатураға қолдануға болады. Триггер механизмдері қарапайым немесе күрделі болуы мүмкін. Әрбір IPS сигнатура әрекеттерін іске қосу үшін осы негізгі триггерлердің біреуін немесе бірнешеуін қолданатын сигнатураларды қамтиды.

Тағы бір кең таралған тетік - бұл протоколды декодтау деп аталады. Пакеттің бір жерінде өрнекті іздеудің орнына, протоколды декодтау пакетті протокол өрістерінде бөліп алады, содан кейін белгілі бір протокол өрісінде немесе басқа өрістердің басқа қателіктерінде іздейді. Хаттаманы декодтаудың артықшылығы - бұл трафикті егжей-тегжейлі тексеруге мүмкіндік береді және ескертуді тудыратын трафик сияқты жалған позитивтердің санын азайтады

2.3.6 IPS енгізудің артықшылықтары. Cisco өзінің Cisco IOS бағдарламалық жасақтамасына IPS мүмкіндіктерін енгізді. Cisco IOS IPS Cisco IDS және IPS диапазонындағы технологияларды қолданады, соның ішінде Cisco IPS 4200 және жаңа IPS 4300 сериялары, сонымен қатар Cisco Catalyst 6500 сериялы интрузияны анықтау жүйесінің қызметтері модулі (IDSM-2). Әр түрлі Cisco IPS 4200 модельдері көрсетілген.

Cisco IOS IPS пайдалану көптеген артықшылықтарға ие:

- ол қауіпсіздіктің қосымша қабатын қамтамасыз ету үшін негізгі маршруттау инфрақұрылымын пайдаланады;
- Cisco IOS IPS кірістірілген және бағыттаушы платформалардың кең спектрінде жұмыс жасайтындықтан, шабуылдарды желі ішіндегі және одан тыс зиянды трафикті блоктау арқылы тиімді түрде бейтараптандыруға болады;
- Cisco IDS, Cisco IOS Firewall, VPN және Network Admission Control (NAC) бірге қолданған кезде, Cisco IOS IPS желінің барлық кіру нүктелерінде қауіптен қорғауды қамтамасыз етеді;
- оған Cisco Configuration Professional сияқты қарапайым және қуатты басқару құралдары қолдау көрсетеді;
- құрылғы пайдаланатын сигнатура дерекқорының көлемін роутердің қол жетімді жадының көлеміне бейімдеуге болады.

3 IPS жүйесін конфигурациялау

3.1 Жұмыстың мақсаты

IDS және/немесе IPS енгізу кезінде қол жетімді жүйелердің түрлерін, хост пен желілік тәсілдерді, осы жүйелердің орналасқан жерін, сигнатура санаттарының рөлін және шабуыл анықталған кезде Cisco IOS маршрутизаторының мүмкін болатын әрекеттерін білу маңызды.

Cisco IOS IPS желіге кіруді анықтау сенсоры ретінде жұмыс істейді, олар құрылғы арқылы ағып жатқан кезде пакеттер мен сессияларды бақылайды және Cisco IOS IPS сигнатураларының кез-келгеніне сәйкес келетін әрбір пакетті қарап шығады. Cisco IOS IPS күдікті әрекетті анықтаған кезде, желінің қауіпсіздігі бұзылғанға дейін жауап береді және оқиғаны Cisco IOS syslog хабарламалары немесе Қауіпсіздік құрылғысы оқиғалары алмасу (SDEE) арқылы тіркейді. Желілік әкімші әр түрлі қауіптерге тиісті жауап таңдау үшін Cisco IOS IPS конфигурациялай алады.

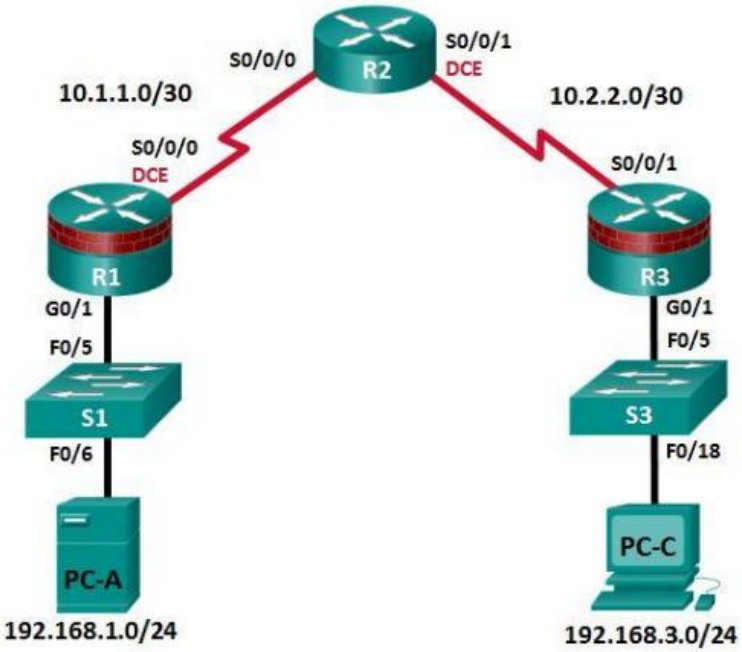
Cisco IOS IPS әкімшілерге маршрутизаторларда кедергілерді болдырмауға мүмкіндік береді. Cisco IOS IPS трафикті белгілі қауіп-қатердің қолдарымен салыстырып, қауіп анықталған кезде бұғаттау арқылы интрузияны бақылайды және болдырмайды.

Бұл жұмыста Cisco IOS желілік мүмкіндіктерінің жиынтығына кіретін Cisco IOS IPS-ті конфигурациялау керек. Интрузияның алдын-алу жүйесі (IPS) шабуылдың нақты үлгілерін және ескертулерін зерттейді немесе олар болған кезде мұндай шабуылдарға қарсы тұрады. Маршрутизаторды Интернетке арналған сенімді желілік экранға айналдыру үшін IPS-тің өзі жеткіліксіз, бірақ басқа қауіпсіздік мүмкіндіктерімен бірге тиімді қорғауды ұйымдастыра алуға болады. Cisco IOS CLI көмегімен IPS баптау керек, содан кейін IPS жұмыс істеп тұрғанын тексеру керек. Біз TFTP серверінен IPS қолтаңбалар пакетін жүктейміз және Cisco IOS көмегімен жалпы криптографиялық кілтті баптаймыз.

Бұл жұмыста Cisco IOS Software Release 15.4 (3) M2 бар Cisco 1941 маршрутизаторына арналған командалар мен нәтижелер қолданылады. Барлық маршрутизаторлар мен қосқыштар қалпына келтірілген және іске қосу конфигурациясы жоқ. Құрылатын желі топологиясы 3.1 суретте көрсетілген.

Пайдаланылған ресурстар:

- 3 маршрутизаторлар (Cisco 1941);
- 2 коммутатор (Cisco 2960);
- 2 PC (Windows7), Tftpd32 сервері, Nmap / Zenmap;
- Топология диаграммасында көрсетілгендей сериялық және Ethernet кабельдері;
- Cisco желілік құрылғыларын конфигурациялауға арналған консольді кабельдер.



3.1 сурет - Құрылатын желі топологиясы

3.1 кесте - Құрылатын желі адресациясы

Құрылғы	Интерфейс	IP Адрес	Желі маскасы	Әдепкі шлюз	Коммутатор порты
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

3.2 Маршрутизатордағы негізгі қауіпсіздік шараларын баптау

Желілік трафикті қорғау және кіріс трафигін мұқият тексеру желі қауіпсіздігінің маңызды аспектілері болып табылады. Сыртқы желіге қосылатын жиілік маршрутизаторын қорғау желіні қауіпсіздендірудің маңызды қадамы болып табылады.

Құрылғылардың қатаюы желінің қауіпсіздігін қамтамасыз етудің маңызды міндеті болып табылады. Ол Cisco IOS Command Line Interface (CLI) және Cisco Configuration Professional (CCP) көмегімен маршрутизатор үшін

физикалық қауіпсіздіктің дәлелденген әдістерін және маршрутизаторға әкімшілік қол жеткізуді қорғауды қамтиды. Бұл әдістердің кейбіріне әкімшілік кіруді қорғау, парольді қолдау, виртуалды кірудің кеңейтілген мүмкіндіктерін конфигурациялау және Secure Shell (SSH) енгізу кіреді. Барлық ақпараттық технологиялар қызметкерлерінің инфрақұрылым құрылғыларына бірдей қол жетімділігі болмауы керек, сондықтан қол жетімділік тұрғысынан әкімшілік рөлдерді анықтау инфрақұрылымдық құрылғыларды қорғаудың тағы бір маңызды аспектісі болып табылады.

Ең алдымен, күшті парольдерді пайдалану керек. Әкімші құпия сөздердің күшті парольдерді құруға арналған стандартты нұсқауларға сәйкес болуын қамтамасыз етуі керек. Ұсынымдар парольдегі әріптер, сандар және арнайы таңбалардың тіркесімін қамтуы мүмкін және оның ең аз ұзындығын анықтайды.

Ұсыныстарға сәйкес болу үшін біз артықшылықты режимнің шифрланған паролін өзгертеміз:

R1(config)# enable secret beknur@2020

Парольде кемінде он таңба болуы керек екенін көрсетеміз:

R1(config)# security passwords min-length 10

SSH қосылымдарын іске қосамыз:

Домендік атау ретінде aues-diplom.com көрсетеміз:

R1(config)# ip domain-name aues-diplom.com

SSH арқылы маршрутизаторға қосылу кезінде қолданылатын жергілікті пайдаланушылардың деректер базасында жазбаны жасаймыз. Пароль күшті пароль стандарттарына сәйкес келуі керек және пайдаланушы әкімші деңгейіне кіру құқығына ие болуы керек:

R1(config)# username admin privilege 15 secret beknur@2020

Vty желілері үшін көлік кірісін тек SSH арқылы қосылыстарды қабылдай алатын етіп теңшейміз, тек «Telnet» -тен басқа:

R1(config)# line vty 0 4
R1(config-line)# transport input ssh

Аутентификация үшін vty линияларында жергілікті пайдаланушының дерекқорын пайдалану керек:

```
R1(config-line)# login local
R1(config-line)# exit
```

Ұзындығы 1024 бит болатын RSA шифрлау кілтін жасаймыз:

```
R1(config)# crypto key generate rsa modulus 1024
```

Кілттердің атауы болады: R1.aues-diplom.com

```
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
 [OK] (elapsed time was 2 seconds)

R1(config)#
*Mar 8 17:54:16.127: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

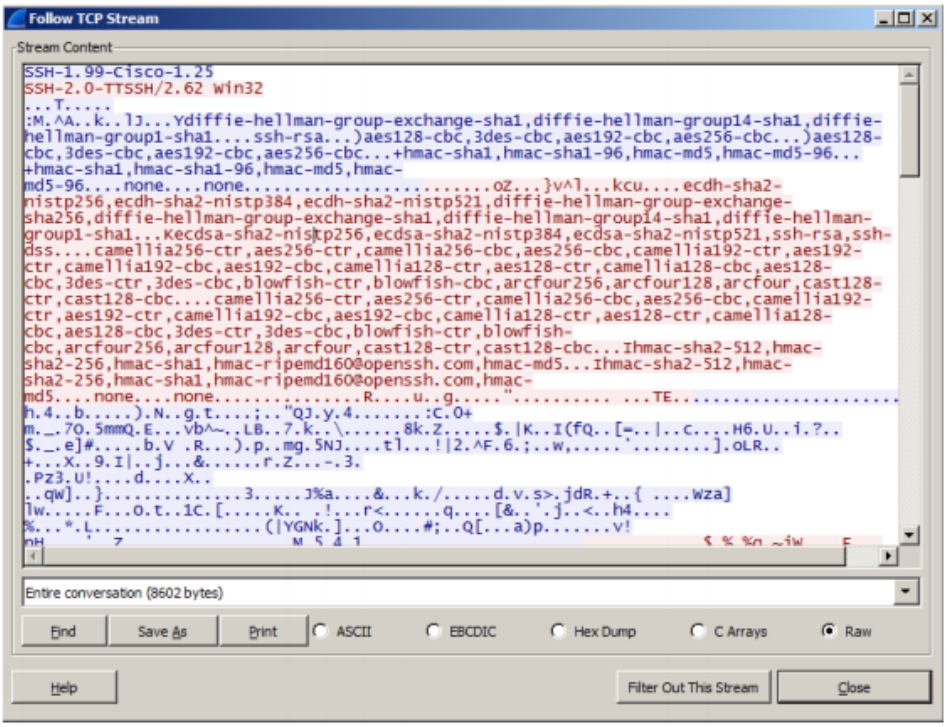
Консоль мен vty линияларын қорғауды қамтамасыз ету. Маршрутизаторды белгілі бір уақыт ішінде белсенді емес қосылым сеансын аяқтауға конфигурациялауға болады. Егер желі әкімшісі желі құрылғысына кіріп, кенеттен басқа жерге шақырылса, белгіленген уақыт өткеннен кейін, бұл пәрмен автоматты түрде қосылу сеансын аяқтайды. Келесі командалар бес минут әрекетсіздіктен кейін сілтемені жабады:

```
R1(config)# line console 0
R1(config-line)# exec-timeout 5 0
R1(config-line)# line vty 0 4
R1(config-line)# exec-timeout 5 0
R1(config-line)# exit
R1(config)#
```

Төмендегі пәрмен толық күш қолдану әдісін қолдана отырып кіруге жол бермейді. Егер қате пароль 120 секунд ішінде екі рет енгізілсе, маршрутизатор кіру әрекеттерін 30 секундқа блоктайды:

```
R1(config)# login block-for 30 attempts 2 within 120
```

SSH артықшылықтарын көрсету үшін Wireshark-тегі TCP мүмкіндігін пайдаланамыз. Wireshark бағдарламасының Пакеттік тізім бөліміндегі SSHv2 жолдарының біреуін тінтуірдің оң жақ түймесімен басамыз және ашылмалы тізімнен Follow TCP ағымының элементін таңдаймыз. SSH сеансының Follow TCP ағымдық терезесін зерттейміз. Деректердің шифрланған және оқылмайтындығын көреміз (3.2-сурет).



3.2 сурет - SSH сеансының Follow TCP Stream терезесі

3.3 Cisco IOS CLI көмегімен IPS-ті конфигурациялау

Біз R1 флэш-жадында IPS каталогын жасаймыз, онда қажетті сигнатура және конфигурация файлдары сақталады:

R1# mkdir ipsdir
Create directory filename [ipsdir]? <Enter>
Created dir flash:ipsdir

IPS криптографиялық кілтін баптау. Криптографиялық кілт басты сигнатура файлының сандық сигнатурасын тексереді (sigdef-default.xml). Әр шығарылымның түпнұсқалығын және тұтастығын қамтамасыз ету үшін мазмұнға Cisco жеке кілтімен қол қойылады.

R1-ге криптографиялық кілт файлын көшіремізз. Ғаламдық конфигурация режимінде криптографиялық кілт файлын таңдап, көшіріп аламыз:

realm-cisco.pub.key.txt.
crypto key pubkey-chain rsa
named-key realm-cisco.pub signature
key-string
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 0282010100C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16 17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128 B199ABCB D34ED0F9 085FADC1

359C189E F30AF10A C0EFB624 7E0764BF 3E53053E5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B8550437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3F3020301 0001

quit

R1 маршрутизаторындағы артықшылықты режимде біз conf командасын қолданып ғаламдық конфигурация режиміне кіреміз. Жаһандық параметрлер режиміне сұранысқа криптографиялық кілттің мазмұнын қоямыз:

R1(config)#
R1(config)# crypto key pubkey-chain rsa
R1(config-pubkey-chain)# named-key realm-cisco.pub signature
R1(config-pubkey-key)# key-string
Enter a public key as a hexidecimal number ....
R1(config-pubkey)#$2A864886 F70D0101 01050003 82010F00 3082010A 02820101
R1(config-pubkey)#$D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
R1(config-pubkey)#$912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
R1(config-pubkey)#$085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
R1(config-pubkey)#$0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
R1(config-pubkey)#$994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
R1(config-pubkey)#$5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
R1(config-pubkey)#$A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
R1(config-pubkey)#$80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
R1(config-pubkey)# F3020301 0001
R1(config-pubkey)# quit
R1(config-pubkey-key)#

IPS ережесін жасау. R1-де ғаламдық конфигурация режимінде ip ips атауының командасын қолданып IPS ереже атауын жасаймыз. IPS ережесінің iosips деп атаймыз. Ол кейінірек интерфейсте IPS қосу үшін қолданылады:

R1(config)# ip ips name iosips

Маршрутизатордың флэш-жадында IPS стгнатура қоймасының орнын көрсетіңіз IPS файлдары ipsdir каталогында сақталады. IP ips config location пәрменін пайдаланып оның орнын көрсеміз:

R1(config)# ip ips config location flash:ipsdir

Бізде IPS-ке Syslog қолдауы бар. Syslog IOS IPS оқиғасы туралы хабарлама жіберу үшін қолданылады. Егер консоль журналы қосылған болса, IPS Syslog журналының хабарламалары көрсетіледі. Sslog бағдарламасын қосу үшін келесі пәрменді пайдаланамыз:

R1(config)# ip ips notify log

Show clock пәрменін пайдаланып, маршрутизатордың ағымдағы уақыты мен күнін тексереміз. Содан кейін артықшылықты режимде clock set пәрменін қолданып сағатты қалпына келтіріп, уақытты орнатамыз

R1# clock set 01:20:00 8 march 2020

Маршрутизаторға show run пәрменін қолданып кіру үшін уақыт белгісі қызметін қосамыз:

R1(config)# service timestamps log datetime msec

Syslog серверіне PC-A серверіне хабарлама жіберу үшін келесі пәрменді пайдаланамыз:

R1(config)# logging 192.168.1.3

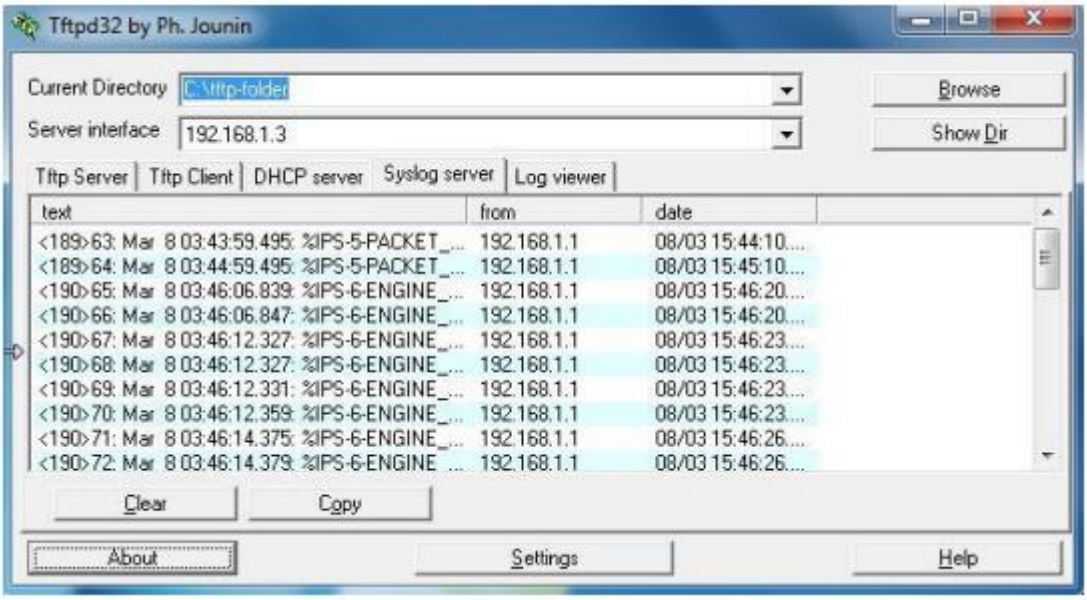
IOS IPS-ті алдын ала анықталған қолтаңба санаттарының біреуін пайдалану үшін конфигурациялау. Cisco 5.x форматындағы сигнатуралары бар IOS IPS басқа Cisco IPS құрылғыларындағыдай сигнатура санаттарымен жұмыс істейді. Барлық сигнатура алдын-ала санатқа бөлінген, ал санаттардың өздері иерархиялық құрылымға ие. Бұл оңай орнату және топтау үшін сигнатураларды жіктеуге мүмкіндік береді.

Сигнатура санатында all сигнатураны шығаруда барлық сигнатураларды қамтиды. IOS IPS шығарылымдағы барлық сигнатураларды бір уақытта жинай және қолдана алмайды. Маршрутизатор үшін жад жеткіліксіз. Сондықтан, IOS IPS-ті конфигурациялау кезінде алдымен all санатындағы барлық сигнатураларды алып тастау керек, содан кейін таңдалған сигнатура санаттарын пайдалану үшін қайтару керек:

```
R1(config)# ip ips signature-category
R1(config-ips-category)# category all
R1(config-ips-category-action)# retired true
R1(config-ips-category-action)# exit
R1(config-ips-category)# category ios_ips basic
R1(config-ips-category-action)# retired false
R1(config-ips-category-action)# exit
R1(config-ips-category)# exit
Do you want to accept these changes? [confirm] <Enter>
```

IPS ережесін интерфейске конфигурация режимінде ip ips атауының бағыттау командасын қолдану. Жаңадан жасалған ережені S0/ 0/0 интерфейсіндегі кіріс трафигі үшін қолданамыз. IPS қосқаннан кейін кейбір журнал хабарламалары консоль жолына жіберіледі. Бұл IPS тетіктері іске қосылатындығын білдіреді.

Бағыт IPS жүйесі интерфейске кіретін трафикті тексереді дегенді білдіреді. Сол сияқты, шығу бағыты тек интерфейстен келетін трафикті білдіреді.



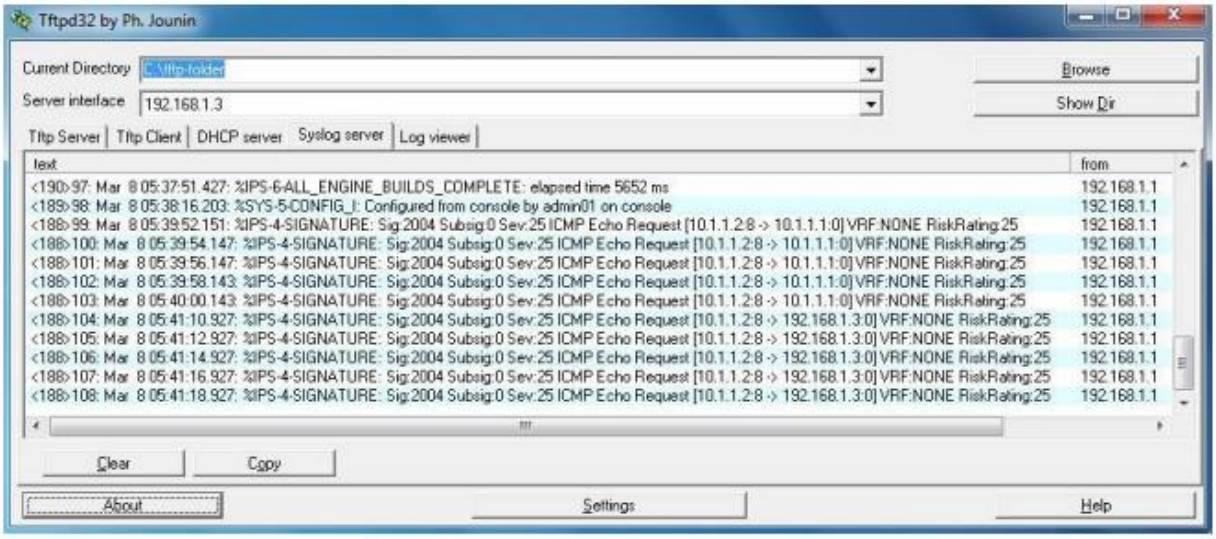
3.3 сурет - Syslog серверіндегі логтар журналы

R1-нің Fa0 / 1 интерфейсі ішкі болғанымен, IPS көмегімен ішкі шабуылдарға жауап беру үшін IPS-ті конфигурациялаймыз. Біз IPS ережесін R1 интерфейсіне Fa1 / 1 интерфейсіне кіріс бағытына қарай қолданамыз:

```
R1(config)# interface g0/1
R1(config-if)# ip ips iosips in
```

Біз эхо сұрау сигнатурасын пайдалану үшін қайтарамыз, оны қосамыз, хабарламадағы қолдың әсерін өзгертеміз, сонымен қатар 0 идентификаторы бар 2004 сигнатурасы үшін қабылдамаймыз және қалпына келтіреміз:

```
R1(config)# ip ips signature-definition
R1(config-sigdef)# signature 2004 0
R1(config-sigdef-sig)#status
R1(config-sigdef-sig-status)# retired false
R1(config-sigdef-sig-status)# enabled true
R1(config-sigdef-sig-status)# engine
R1(config-sigdef-sig-engine)# event-action produce-alert
R1(config-sigdef-sig-engine)# event-action deny-packet-inline
R1(config-sigdef-sig-engine)# event-action reset-tcp-connection
R1(config-sigdef-sig-engine)# exit
R1(config-sigdef-sig)# exit
R1(config-sigdef)# exit
Do you want to accept these changes? [confirm] <Enter>
```



3.4 сурет - 2004 0 (ICMP) сигнатурасын қосқаннан кейінгі Syslog серверіндегі логтар журналы

3.4 Шабуыл иммитациясы

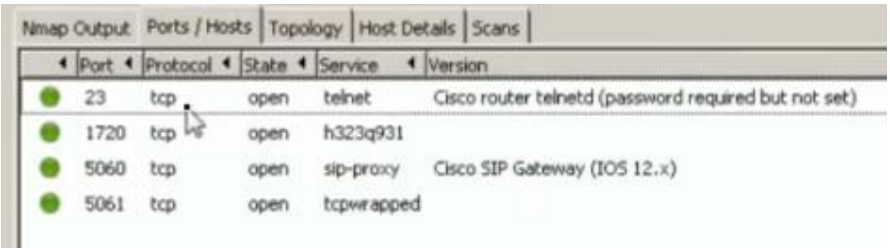
Nmap / Zenmap - бұл желінің хосттары мен ресурстарын, соның ішінде қызметтерді, порттарды, операциялық жүйелерді және саусақ ізі туралы басқа ақпаратты анықтайтын желіні қарап шығу құралы. Zenmap - Nmap үшін графикалық интерфейс. Nmap алдын-ала рұқсатынсыз желіні қарап шығу үшін пайдаланылмауы керек. Желіні қарап шығу фактісін желілік шабуылдың бір түрі ретінде қабылдауға болады.

Nmap / Zenmap R1-де IPS мүмкіндіктерін сынайды. Біз PC-A-де сканерлеу бағдарламасын іске қосамыз және R1 маршрутизаторында IPS

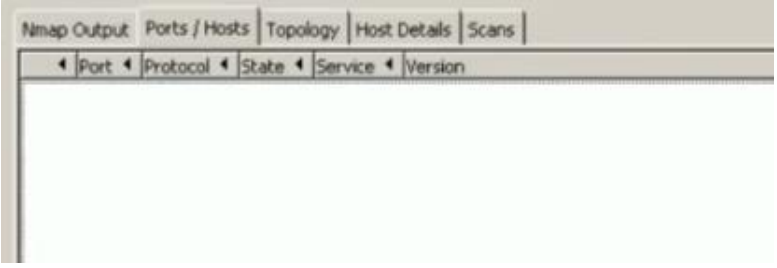
iosips ережесін қолданғанға дейін және кейін R2 маршрутизаторындағы ашық порттарды сканерлеуге тырысамыз.

PC-A-де Zenmap іске қосамыз. Target өрісіне 10.1.1.2 IP мекенжайын енгізіп, Profile өрісінде Intense Scan таңдаймыз. Сканерлеуді бастау үшін Scan түймесін басамыз.

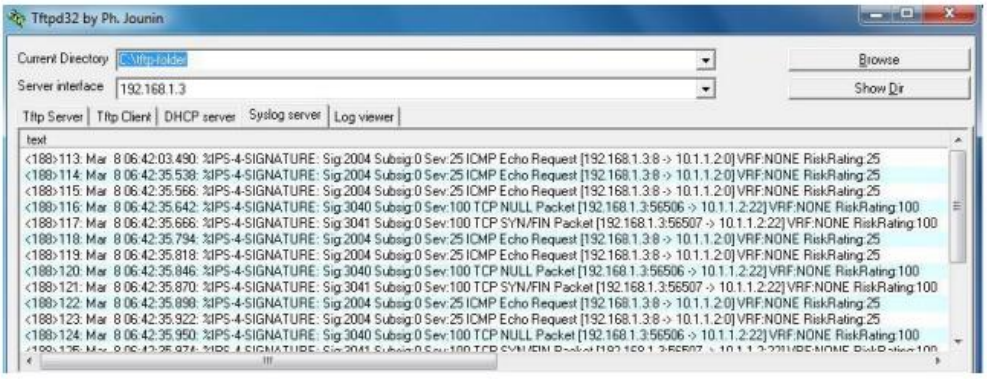
Біз IPS ережелерін қолданбаған кезде сканер бізге R2 маршрутизаторының барлық порттан көрсетіп берді (3.5 сурет). Ал ережелерді орнатқаннан кейін еш порт көрсетілмеді (3.6 сурет). Ал шабуыл жасау әрекетін Syslog серверінде аңғарсақ болады (3.7 сурет). TCP NULL Packet және TCP SYN/FIN Packet.логтарын көре аламыз.



3.5 сурет - IPS ережелерін қолданбас бұрын портты сканерлеу нәтижесі



3.6 сурет - IPS ережелерін қолданнан кейінгі портты сканерлеу нәтижесі



3.7 сурет - Nmap / Zenmap арқылы портты сканерлеу шабуылынан кейін Syslog серверіндегі логтар журналы

IPS енуді анықтау және алдын-алу шешімдерін енгізу бірнеше артықшылықтарға ие:

- In-Line режимінде немесе жедел режимде жұмыс істеу мүмкіндігі - лезде сүзгілеуді қамтамасыз ету;

- анықтаудың әртүрлі әдістерін қолдану - қолды талдау, мінез-құлықты талдау, ауытқулар мен ауытқуларды анықтау, эвристикалық талдау;

- белгілі де белгісіз шабуылдардың алдын-алу - «нөлдік шабуылдар»;

- қолдар мен бағдарламалық жасақтаманы үнемі жаңартып отыру;

- қолдарды икемді түрде конфигурациялау, жаңаларын құру мүмкіндігі;

- виртуализацияны қолдау, түрлі байланыс арналары / желілік бөлімдері / клиенттері үшін әр түрлі қауіпсіздік саясатын қолдану мүмкіндігі;

- АҚ оқиғаларын орталықтандырылған басқару және бақылау, есептер шығару мүмкіндігі.

4 Өміртіршілік қауіпсіздігі

4.1 Еңбек жағдайын талдау

Бұл дипломдық жоба IPS басып кіруді ерте анықтау жүйесі қарастырылды.

Қалыпты жұмыс жағдайларын және техникалық талаптарды қамтамасыз ету тұрғысынан ол мыналарға ие: жұмыс орнын жеткілікті жарықтандыру; жабдықтың толық жарамдылығы, оның электр қауіпсіздігі; бөлменің жеткілікті өрт қауіпсіздігі; өнімді жұмыс пен жұмыс орнының эргономикалық талаптарға сәйкес келуіне ықпал ететін қолайлы микроклимат. Жұмысшылар ұшырайтын қауіпті және зиянды еңбек жағдайларына мыналарды жатқызуға болады: электр тогының соғуы, электр жабдықтарының жұмыс істемеуі, қауіпсіздік ережелерін сақтамау немесе жерге тұйықтау бұзылуы; қолайсыз параметрлері бар микроклиматта жұмыс істеу; жұмыс орнын жеткіліксіз жарықтандырумен жұмыс.

Жабдық келесі жағдайларда оңтайлы жұмыс істейді:

- температура 0-ден 40 °қа дейін;

- ылғалдылық 5-тен 95% -ға дейін, конденсацияланбаған;

- қуат: ауыспалы ток - кернеуі 100-ден 220 В-қа дейін, жиілігі 50 / 60Гц, ток 2 - 5 А ; DC - кернеу 48-ден 60 В-қа дейін, жүктеме тогы 2 - 4 А.

Барлық арнайы жабдықтардың сертификаттары болғандықтан, бұл жағдайда кәсіби қауіп-қатерлер класы ең кіші болып анықталады.

Электрлік құрылғыларды жұмыс кернеуі 1 кВ дейінгі жабдыққа жатқызуға болады.

Электр тогының соғу қаупі деңгейіне сәйкес бөлмені жоғары қауіптіліксіз жіктеуге болады, өйткені ол:

- жеткілікті ылғалдылық;

- қолайлы микроклиматпен;

- оқшауланған едендермен;

- шаңсыз;

- жерге тұйықталған заттар жоқ.

Қоршаған ортаның табиғатына сәйкес жұмыс бөлмесін «қалыпты құрғақ» деп бөлуге болады, орташа ылғалдылық 60% -дан аспайды. Рұқсат етілген мән деңгейіне сәйкес, ол электр санатына жатады, яғни техникалық жабдыққа қол жеткізуді тек электр мамандары жүзеге асырады. Электр қондырғыларына эксплуатациялық қызмет көрсетуді кезекші персонал жүзеге асырады, олардың біліктілігі жоғары топ III топтан төмен емес .

Жүргізіліп жатқан процестің сипаттамалық сипаты, қолданылатын элементтер мен материалдардың қасиеттері, сондай-ақ электр қондырғыларының, базалық станция жабдықтары орнатылатын үй-жайлардың болуы өрт қауіптілігі D санатына жатады, ал II - IIа класына жатады . Осылайша, бөлменің кейбір әрлеу, сәндік материалдары (түрлі жасанды қосылыстар, полимерлер). Өрттің себебі қысқа тұйықталу немесе қуат кабелінің зақымдануы болуы мүмкін.

Серверлік бөлмедегі әрекеттерді қалыпты жұмысқа жатқызуға болады, өйткені техникалық жабдық әр түрлі енгізу/шығару құрылғыларынан қашықтан басқарылады: компьютерлер, принтерлер, модемдер, маршрутизаторлар, маршрутизаторлар.

Жұмыс орнын ұйымдастыру заманауи эргономикалық стандарттарға негізделген. Жұмыс жасайтын жиһаздың дизайны (үстелдер мен орындықтар) қызметкердің өсуіне сәйкес жеке түзетуге мүмкіндік береді және ыңғайлы жағдай жасайды. Жиі қолданылатын еңбек құралдары мен басқару элементтері оңтайлы жұмыс аймағында.

Орындықта жұмысты орындауға арналған жұмыс орны ГОСТ талаптарына сәйкес келеді [21]**.** Оның элементтері жүйесінде біз іс-әрекеттің сипатын, адамның өзіне тән ерекшеліктерін және оның физикалық деректерін ескереміз.

Жұмыс бөлмесінде келесі өлшемдер бар: ұзындығы A = 10 м, бөлменің ені B = 5 м, биіктігі H = 3 м, еденнен жоғары жұмыс алаңының биіктігі - 1,2 м, терезелер 0,8 м биіктіктен басталады, терезелердің биіктігі 1м, маңайдағы ғимарат - 10 м қашықтықтағы ғимарат, биіктігі 7 м, екінші жағынан көлеңкелі құрылымдар жоқ.

Бөлмеде келесі телекоммуникациялық жабдық орналасқан:

- кондиционер;
- сейф;
- администратор орны ;
- жабдықталған серверлік шкафпен;
- лазерлік MFP.

Жабдықтардың орналасуы 4.1 суретте көрсетілген.

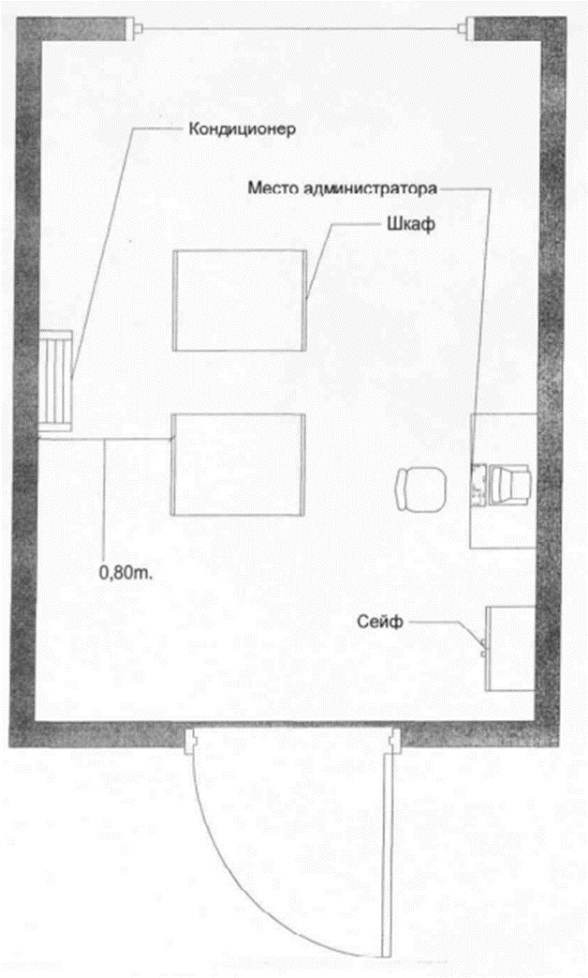
Серверлік бөлмеде ГОСТ [9] талаптарына сәйкес 1 қызметкер болады, бір адамға шаққанда кемінде 6,5 м^2 алаң болуы керек. Серверлік бөлменің ауданы 50 м^2 құрайды, оның 2 м^2 жабдық шкафтарымен жабдықталған, демек, бір қызметкерге бөлме алаңының 16 м^2 талаптарға сай келеді.

Бір ДК шығаратын шу аз, ол 30-68 дБ диапазонында. ГОСТ 12.1.003-83 [10] сәйкес ол 40 дБ деңгейінен аспауы керек. Бірақ онда бір компьютер болғандықтан, ол шығарған шу осы талаптарға сай келеді.

Апаттық жарықтандырудың қуаты мен басқару орталық апаттық жарықтандыру жүйесінен қамтамасыз етіледі. Сонымен қатар, қалыпты режимде сәйкес лампалар номиналды мәннен 100% жарқыраған ағынды қамтамасыз етеді, ал апаттық режимде (орталық батареядан жұмыс жасағанда) - 25% (деңгей бағдарламаланған).

Сервер бөлмесінде маңызды деректердің резервтік көшірмесін сақтау үшін сейф орналастырылды.

Сервер бөлмесіне кіру шектеуленген. Алдыңғы есікке шектеулі қол жетімділікті қамтамасыз ету үшін код құлпы орнатылды.



4.1 сурет - Сервер бөлмесінде жабдықтар мен жұмыс орындарын орналастыру жоспары

4.1.1 Өрт қауіпсіздігі. Сервер бөлмесінің ауданы 24 м² асатындықтан, СН 512-78 [11] стандартына негізделген автоматты газды сөндіру қондырғысымен жабдықталған.

Сервер бөлмесі - бұл қымбат серверлік жабдықтары бар тіректер орнатылатын объектілер. Есептеу техникасы мен сақтау жүйелерінің зақымдануы иеленуші компанияға тікелей шығындарды ғана емес, сонымен қатар маңызды коммерциялық ақпаратты жоғалтуға әкеледі. Сондықтан, сервер аймағындағы өртті сөндіру үшін әрқашан тек газды сөндіру әдісі қолданылады. Бұл әдіспен деректер орталығының желісіне және есептеу ресурстарына әсер етілмейді. Сервер бөлмесі автоматты өрт дабылымен жабдықталған. Автоматты өрт дабылы түтінге жауап беретін өртті ерте анықтауға арналған датчиктермен жабдықталған.

Сервер бөлмесі басқа бөлмелерден отқа төзімділік рейтингісі 0,75 сағатты құрайтын бөлімдермен бөлінген, ал есіктер отқа төзімділік рейтингісі - 0,8 сағатты құрайды. Қабырғалар мен есіктер су өткізбейтін - бұл тек өрт кезінде ғана емес, сонымен қатар микроклиматты сақтау үшін де пайдалы.

Өрт сөндіру үшін кәсіпорындар әртүрлі схемалар мен құрылғылардың түрлерін, сондай-ақ олардың комбинацияларын қолданады. Газды өрт сөндіру жұмсақ жұмсақ әдіске жатады, оның ішінде үй-жайлардың іші мен оған орнатылған жабдықтар зардап шекпейді.

Модульдік автоматты газды сөндіру қондырғылары. Функционалды мақсаты:

- от пен түтінді анықтау және сөндіру;
- деректер орталығының менеджеріне өрт сигналын беру;
- қондырғының жұмыс күйін бақылау.

Орнату компоненттері:

- GOTV жеткізуге арналған құбыр;
- әртүрлі типтегі саптамалардың жиынтығы;
- іске қосу модулінің құлыптау және іске қосу құрылғысын ашуға арналған импульс тудыратын электр модульдері;
- газды сөндіргішті (GOTV) сақтауға және босатуға арналған өрт сөндіру модульдері.

Серверлік бөлмелерде өрт сөндіру жүйелеріне арналған HFC газдары. Әр түрлі өндірушілердің модульді автоматты газды өрт сөндіру қондырғыларында әр түрлі өрт сөндіру құралдары қолданылады. GOTV түрі автоматты орнатудың нақты өндірушісіне байланысты.

Көбінесе салқындатқыш газдар GOTV ретінде қолданылады. Фреондар - жану ингибиторлары және өрт кезінде химиялық процестерді белсенді тежейді. Фреон 125 (C2F5H) - ауадағы аз концентрациядағы газ (9% дейін) адам өмірі үшін қауіпсіз.

Осы қасиетті ескере отырып, кладондар Екінші дүниежүзілік соғыстан ертеде әскери снарядтармен жарылған әскери техникалар мен танктерді сөндіру үшін қолданылды.

Inergen Freon - бұл азот, аргон және көмірқышқыл газының газ қоспасы. Ингерген бөлмеде оттегін сіңіру арқылы өртті сөндіреді.

Қауіпсіздік мақсатында инергенді сақтау цилиндрі өте жоғары қысымға ие болуы керек (300 бар). Ұзақ мерзімді сақтау кезінде бұл цилиндр

корпусының тығыздығының бұзылуына және газдың ағып кетуіне әкелуі мүмкін. Нысанда жоғары сапалы өрт сөндіру үшін жоғары мөлшерде инерген концентрациясы бар цилиндрлер және оларды сақтау үшін арнайы орын қажет.

Novec ™ 1230 (C-6 фторокетон) сервер үшін таңдалды - B, C, D және E сыныпты өртті сөндіру үшін заманауи өрт сөндіру жүйелерінде қолданылатын 3M корпорациясының патенттелген дамуы.

4.2 сурет - Novec™ 1230 өрт сөндіргіші

Пайдалы ерекшеліктері:

- адам денсаулығына зиянды әсер етпейді;
- бөлмедегі оттегінің концентрациясына әсер етпейді;
- құрамында бром және хлор молекулалары жоқ, сондықтан ол қоршаған орта үшін қауіпсіз;
- тікелей күн сәулесінің әсерінен 5 күн ішінде субстанцияның толық өздігінен ыдырауы;
- жылуды судан бірнеше есе жақсы сіңіреді;
- электростатикалық қасиетке ие емес, сондықтан электроникаға әсер етпейді;
- ол сұйық түрінде оңай тасымалданады: қысымсыз, «қауіпті жүктерді» таңбасыз;
- орнына цилиндрлерді тез толтыру мүмкіндігі.

4.1.2 Микроклимат. Жұмыс істеп тұрған жабдық үнемі үлкен көлемде жылуды шығарады, ал кондиционерлер болмаған жағдайда қызып кету мүмкін емес. Оның салдары өте жағымсыз - аппараттық ақаулардан бастап қызмет мерзімін қысқартуға дейін (жұмыс температурасын 10 градусқа көтеру жабдықтың қызмет ету мерзімін екі есе қысқартады деген пікір бар).

Сондықтан сервер бөлмесінде қалыпты жұмыс істеу үшін температура 18-ден 24 ° С-қа дейін болады.

Температурадан басқа, салыстырмалы ылғалдылық деңгейін бақылау қажет. Жоғары ылғалдылық конденсаттың пайда болуына қауіп төндіреді, ал ол өз кезегінде коррозияға ұшырайды. Құрғақ ауа проблемалар туғызбайды: төмен ылғалдылық жағдайында заттар электрониканы зақымдауы мүмкін статикалық электр қуатын оңай жинайды. Сонымен қатар, кешіктірілген ауа жылуды нашар таратады. Дәл сол TIA / EIA-569 [12] сервер бөлмесінде салыстырмалы ылғалдылықтың оңтайлы деңгейі 30-50% құрайды.

Қажетті микроклиматты дәлме-дәл кондиционерлермен ұстаған дұрыс: олар температураны 1°С дәлдікпен орнатуға, ылғалдылық пен таза ауаны реттеуге мүмкіндік береді. Сервер бөлмесіне арналған кондиционер жүйесі кем дегенде бір резервтік құрылғыны қамтуы керек: егер бір кондиционер бұзылса, резервтік температураның көтерілуіне жол бермейді.

Біздің серверлік бөлмеміз үшін сыртқы ауамен салқындатылатын конденсаторы бар және ауа температурасы төмен желдеткіш AM SDAC 0251A дәлме-дәл кондиционері таңдалған. Кондиционер орталықтан тепкіш желдеткіштермен жабдықталған, олар жоғары өнімділікпен және жұмыс кезінде шу деңгейінің төмендеуімен сипатталады.

Uniflair AM SDAC 0251A дәлме-дәл кондиционерлерінің негізгі мақсаты - бөлмеде орнатылған жабдықтардың жұмысына қажетті барлық талаптарға толық жауап беретін микроклимат жасау. Жабдықтардың бұл түрі, әдетте, жоғары дәлдіктегі жабдықты қамтиды, оларды пайдалану үшін белгілі бір климаттық жағдайлар қажет, ал үй-жайлар әртүрлі болуы мүмкін: медициналық пункттер, бақылау-өткізу пункттері, серверлік бөлмелер. Бұл сонымен қатар әртүрлі мұрағаттар немесе кітапханалар болуы мүмкін, мұнда кітаптарды немесе құжаттарды сақтау шарттарын сақтау қажет.

4.3-сурет - AM SDAC 0251A дәлме-дәл кондиционері

Кондиционер корпусының тереңдігі 45 см тереңдікте, сонымен қатар корпустың ішкі элементтері мен кондиционерді бөлімдерге бөлетін ішкі

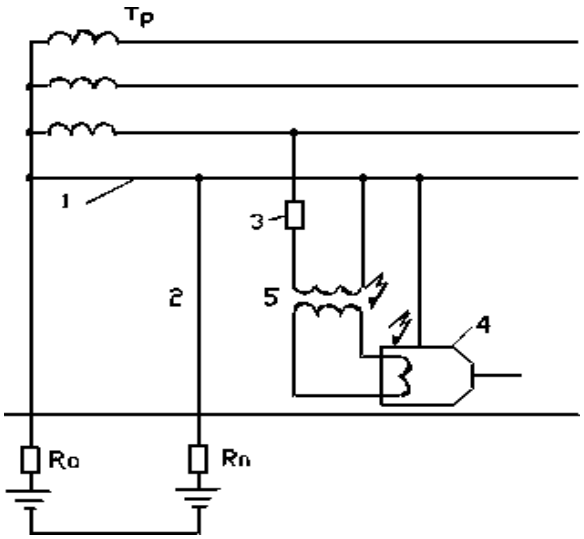
панельдер мырышталған парақтан жасалған, бұл жалпы құрылымды мүмкіндігінше күшті етеді.

Uniflair AM SDAC 0251A кондиционерінің негізгі сипаттамалары мен ерекшеліктері:

- жұмыс кезінде пайда болатын қондырғының жылуын кетіретін қашықтағы конденсатор;
- ауа қабылдау - жоғарыдан (міндетті түрде алдыңғы), үрлеу - төмен қарай;
- ауа сүзгісі;
- ауаны ластау сенсоры;
- герметикалық айналдыру компрессоры;
- компрессорға енгізілген діріл қондырғылары мен термиялық қорғаныс;
- буландырғыш - алюминий қыртысы бар мыс түтіктер;
- науа баспайтын болаттан жасалған;
- конденсатты ағызу үшін арнайы икемді шланг қарастырылған.

4.1.3 Жұмыс жағдайындағы жерге тұйықтау. Лабораторияда көптеген электрқондырғылар бар болатындықтан, яғни серверлер мен компьютерлер, әрі олардың тіреулері металдан жасалғандықтан, ол жерде міндетті түрде жерге тұйықтау болуы тиіс.

Жерге тұйықтау кернеуі төртөткізгіштік электрсызықтарында жерге тұйықтау нейтралының 1000В дейінгісі қолданылады. Жерге тұйықтауды қорғау электрқондырғының зақымдалған жерінің автоматты түрде өшірілуі электрсызығынан немесе кернеуді төмендету арқылы қамтамасыз етіледі. Жоғарыда айтылғандарды қорытындылай келе, жерге тұйықтаудың басты мақсаты корпустағы тұйықталу кезінде токтан мак максималды қорғау болып табылады. Ол үшін қысқа тұйықталу тогы балқушы құрылғылардың номиналды тогынан бірнеше есе үлкен болуы керек. 4.4 суретте жерге тұйықтаудың принципиалды сызбанұсқасы келтірілген.



4.4 сурет - Жерге тұйықтау сызбанұсқасы. Ro – жерге тұйықтаудың бейтарап кернеуі; Rh – адамның есептік кедергісі; 1-

жерге тұйықтау магистралі; 2- қайтадан жерге тұйықтау магистралі; 3- өшіру аппараты; 4- электрқондырғы; 5- трансформатор.

Ток күші қосымша жалғанған кернеу мөлшері мен дене аймағының кедергісіне байланысты болады. дене аймағының кедергісі ішкі мүшелер жасушаларының кедергісінен және тері кедергісінен қалыптасады. Есептеу барысында R= 1000Ом. Әртүрлі мөлшердегі токтың әсер етуі 4.1 кестеде келтірілген.

4.1 кесте. Әртүрлі мөлшердегі токтың әсер етуі

Ток, мА	Адамға әсер етуі	
	Ауыспалы ток	Тұрақты ток
0,5	Болмайды	Болмайды
0,6-1,5	Саусақтардың әлсіз дірілдеуі	Болмайды
2-3	Саусақтардың қатты дірілдеуі	Болмайды
5-10	Қолдың тартылуы	Күйдіру
12-15	Сымнан қолды тартып алу қиын	Қатты күйдіру
20-25	Қол біртіндеп жансызданады	Қатты күйдіру
50-80	Тыныс алудың тоқтауы	Тыныс алудың қиындауы
90-100	t>3 сек жоғары – жүректің тоқтауы	Тыныс алу тоқтауы

Оларды қолдану кезінде ауыспалы және тұрақты токтың электрқондырғыларының қауіпсіздік техникасына бірдей талаптар қойылады.

4.2 Есептеу бөлімі

4.2.1 Жерге тұйықтау процесін есептеу әдістері. Жерге тұйықтау процесі [13] әдістемелік нұсқауға сәйкес есептейміз. 220В номиналды кернеуі бар және 10А номиналды тогы бар электрқондырғыларын нөлге теңестіру жобалануда.

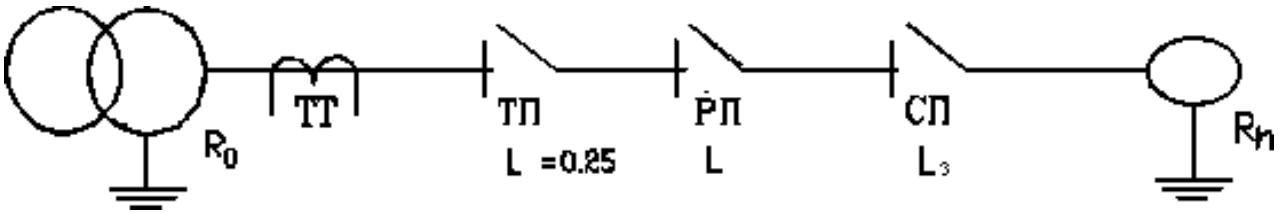
Электрқондырғыны қуаттандыру үшін лабораториялық күштік жиынтықты болаттан жасалған түтікшеге орналастырылған АЛП маркалы сым қолданылады. Көлденең қимасы S=2.5мм^2 болатын алюминий өткізгішін таңдаймыз. Тұтынушы магистралдың үшінші бөлігімен жалғастырылған.

Магистралдың бірінші бөлімі полихлорвинилді қабықшада (3 *50 + 1*25), енді көлденең қимасы бар алюминий сымдары АВРЕ маркалы төртсымды кабельмен орындалған. Бірінші бөлімнің ұзындығы - 0,25 км. Іном = 100А бөлімі токтың А 3110 таратушысы бар автоматпен қорғалған.

Екінші бөлімі ұзындығы 0,075 километр болатын АВРЕ (3 *25 + 1*10) мм кабелімен салынған. Бөлім 80А тогы бар А 3134 автоматты рубильнигімен қорғалған. Магистраль бастапқы кернеуі 6кВ дәне екінші кернеуі 400/220В болатын ТМ=1000 типті трансформатордан қуатталады.

Жерге тұйықтаудың орындалған магистралі алғашқы екі бөлімде қуаттаудың төртінші кабелімен орындалған, ал үшінші бөлімінде – болаттан

жасалған түтікше болады.



ТТ – трансформатор; ТП - трансформаторлық подстанция;
РП – таратушы пункт; СП – күштік пункт.

4.5 сурет - Энергия көзінің сызбанұсқасы

Қорғаныс үшін ПР-2 тежегіш (қорғауыш) пайдаланылады. Қорғауыш тогы:

$$I_{\text{пр}} = \frac{3 \cdot K_{\text{П}} \cdot I_H}{2{,}5} = \frac{3 \cdot 10}{2{,}5} = 12A.$$

мұндағы, Кп –қосылу коэффициенті = 0,5...4,0.

К коэффициентінің мәні электрқондырғының типіне байланысты алынады:

- егер қорғаныс бір электромагниттік уақытша қолдауынсыз, автоматты түрде өшірілу арқылы жүргізілетін болса, К 1,25; 1,4 шамасында алынады.
- егер қорғаныс жанып кету уақыты токқа байланысты (ток артқан сайын төмендей бастайды) болатын балқытушы қорғауыштар арқылы жүргізілетін болса, өшіруді жылдамдату мақсатында К 3 алынады.
- егер ток көзіне кері қосылудың автоматты қорғауыштары қорғалған болса, онда К≥3 алынады.

Стандартты қорғауыш 15А таңдаймыз.

Өйткені сызбанұсқада магистраль бөлімі 20 Ом артық болған жағдайда қайтадан жерге тұйықтау қажет. Жерге тұйықтау кедергісі 10 Ом аспау керек.

Трансформатор кедергісінің есептік мәнін анықтаймыз:

$$R = \rho \frac{L}{S}, \tag{4.1}$$

мұндағы, L – сым ұзындығы (м);

S – сымның қимасы (көлденең қимасы, мм^2);

ρ - материалдың салыстырмалы кедергісі (алюминий үшін ρ=0,028 Ом*мм^2/км).

Фазалық сымның үш бөлімінің активті кедергісін есептейміз:

$$R_1 = 0{,}028 \cdot \frac{250}{50} = 0{,}14(\text{Ом}).$$

$$R_2 = 0{,}028 \cdot \frac{75}{25} = 0{,}084(\text{Ом}).$$

$$R_3 = 0{,}028 \cdot \frac{30}{2{,}5} = 0{,}336(\text{Ом}).$$

$R_{Ф1}$=0,14(Ом); $R_{Ф2}$=0,084(Ом); $R_{Ф3}$= 0,336(Ом).

Фазалық сымның толық активті кедергісі: $R_{Ф\Sigma}$ =0,56(Ом);

Сым температурасын T=55C барлық бөлімде бірдей деп қарастырып, температуралық түзетулерді ескере отырып, фазалық өткізудің активті кедергісін есептейміз.

$$R_{Ф} = R_{Ф\Sigma} \cdot \left(1 + a \cdot \left(T - 20\right)\right) = 0{,}64(\text{Ом}).$$

мұндағы, $a = 0{,}004^{-1}$град – алюминийдің кедеріг температуралық коэффициенті.

Нөлдік қорғаныстағы сымның активті кедергісі:

$$\mathrm{R}_{\mathrm{M31}} = 0{,}028 \cdot \frac{250}{25} = 0{,}28(\text{Ом}).$$

$$\mathrm{R}_{\mathrm{M32}} = 0{,}028 \cdot \frac{75}{10} = 0{,}21(\text{Ом}).$$

Болаттан жасалған құбыр үшін: ρ=1,8Ом*мм^2/км

$$\mathrm{R}_{\mathrm{M3}} = 1{,}8 \cdot 30 \cdot 10^{-3} = 0{,}054(\text{Ом}).$$

Осылайша, жерге тұйықтау магистралінің жалпы кедергісі тең болады:

$$R_{M\Sigma} = R_{M\,1} + R_{M\,2} + R_{M\,3} = 0{,}544(\text{Ом}).$$

Фазалық сым үшін ішкі индуктивті кедергісін анықтаймыз.

$$X'_{Ф} = X'_{ФM} - X_{ФL}, \qquad (4.2)$$

Жерге тұйықтау магистралы үшін:

$$X'_{M} = X'_{M\,M} - X_{M\,L}, \qquad (4.3)$$

мұндағы, X'_M және $X'_{ФМ}$- индуктивті кедергі, фазалық сымның және жерге тұйықтау магистралының өзара индуктивті жағдайы;

X_M және $X_{Ф1}$- өзіндік индукцияның ішкі индуктивті кедергісі.

Индуктивті кедергі, фазалық сымның және жерге тұйықтау магистралының өзара индуктивті жағдайы келесі формула бойынша анықталады:

$$X'_{ФМ} = X'_{ММ} = 0145\lg(d_{ФМ}), \quad (4.4)$$

мұндағы, d – фазалық және нөлдік сымдар арасындағы арақашықтық (1 және 2 d=15 мм үшін, 3 d=9.5 мм үшін)

$$X'_{ФМ1}=X'_{ЖММ}=0{,}145\ \lg15=0{,}17(Ом).$$

$$X'_{ФМ2}=X'_{ЖММ}=0{,}145\ \lg15=0{,}17(Ом).$$

$$X'_{ФМ3}=X'_{ЖММ}=0{,}145\ \lg9{,}5=0{,}142(Ом).$$

Барлық территориядағы жалпы кедергі:

$$X'_{ФМ} = X'_{ЖММ} = 3*0{,}145=0{,}482(Ом).$$

Ішкі индуктивті кедергі келесі формула бойынша анықталады:

$$_{ФL} = X'_{L*} L, \quad (4.5)$$

мұндағы, X'_L- жеке индукцияның салыстырмалы кедергісі, Ом/м.

$$X'_{L1} = 0{,}09*0{,}25=0{,}023\ (Ом).$$

$$X'_{L2}=0{,}068*0{,}075=0{,}005\ (Ом).$$

$$X'_{L3} = 0{,}03*0{,}03=0{,}0009\ (Ом).$$

Фазалық сымның жалпы ішкі индуктивті кедергісі:

$$X_{ФL}=0{,}029\ (Ом).$$

$$X_{ML1} = 0{,}068*0{,}25=0{,}017\ (Ом).$$

$$X_{ML2}=0{,}03*0{,}075=0{,}0025(Ом).$$

$$X_{ML3}=0{,}138*0{,}03=0{,}004(Ом).$$

Жерге тұйықтау магистралінің жалпы ішкі индуктивті кедергісі:

$$X_{ML}=0,024(Ом).$$

Жалпы ішкі индуктивті кедергі:

$$X_{Ф}'=0,435-0,0314=0,453(Ом).$$

$$X_{ЖМ}'=0,435-0,0244=0,458(Ом).$$

Ішкі индуктивті кедергіні анықтаймыз:

$$X_{Ф}''_{1-2}= X_{ЖМ}''_{1-2}=0,057*0,075=0,001(Ом).$$

$$X_{Ф}''_{3}=0,0157*0,03=0,0005(Ом).$$

Фазалық сымның және жерге тұйықтау магистралінің толық кедергісі:

$$Z_{Ф}=0,78(Ом).$$

$$Z_{M}=0,79(Ом).$$

Бұл формула бойынша токтың бірфазалығын анықтаймыз:

$$I_{КТ} = \frac{U_{Ф}}{\frac{Z_{Ф}}{3}+Z_{ЖМ}} = \frac{220}{0,78+0,79} = 132A\ , \qquad (4.6)$$

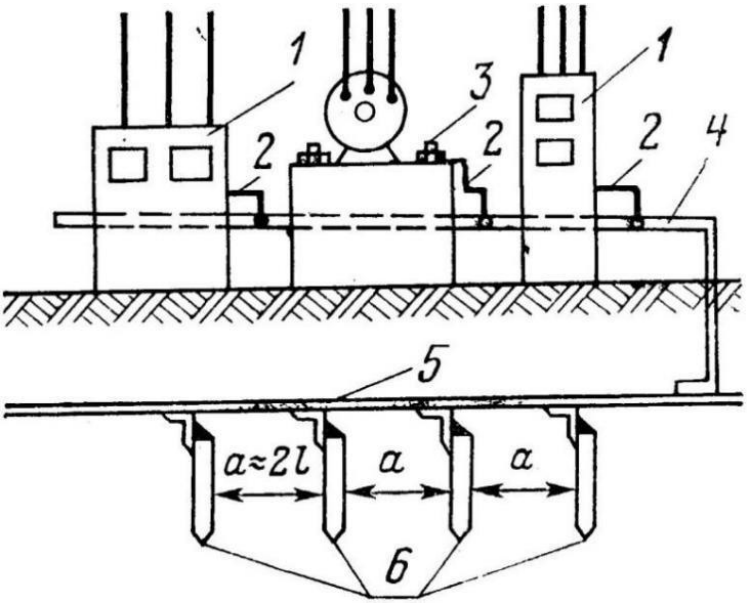
Есептелген көрсеткіш пен рұқсат етілген көрсеткішті салыстырамыз:

$$I_{КЗ}=132>12A.$$

Берілген шарттың орындалуын тексереміз.

$$Z_{M} < 2\text{-}Z_{Ф.}$$

Шарт орындалды.



1- электрқондырғы; 2- жерге тұйықтау өткізгіштері; 3- өткізгіштің орнатылу болты; 4- жерге тұйықтау магистралі; 5- шина контуры; 6- жерге тұйықтаушы (құбыр, бұрыштар).

4.6 сурет - Қорғаныстық жерге тұйықтау конструкциясы

5 Экономикалық бөлім

5.1 Ақпараттық қауіпсіздікті қамтамасыз ету құнын есептеу

Компанияның ақпараттық қауіпсіздігін (АҚ) қамтамасыз ету шығындары, егер олар мемлекеттік нормативтік құжаттар мен стандарттардың, сондай-ақ ақпараттық қауіпсіздік тұжырымдамасының сақталуын қамтамасыз етсе, тиімді болып табылады. Бұл түсінік ақпараттық қауіпсіздіктің экономикалық тиімділігін объективті бағалаудың әмбебап әдістері жоқтығына байланысты. Экономикалық тиімділік, әдетте, тиісті іс-шаралардың түпкілікті нәтижелері бойынша шығындар сметасының есеп айырысу кезеңіндегі оларды жүзеге асыру үшін ресурстардың жалпы құнынан асып түсуі ретінде түсініледі [14].

Ақпараттық қауіпсіздік шараларының тиімділігін бағалаудың күрделілігі бірқатар жағдайларға байланысты. Жүйелердің тиімділігін бағалау теориясына сәйкес, кез-келген объектінің, оның ішінде ақпараттық қауіпсіздік жүйесін (АҚЖ) пайдалану сапасы оны мақсатты пайдалану (мақсатты жұмыс) процесінде ғана көрінеді, сондықтан қолданбаның тиімділігін бағалау объективті болып табылады [14].

Сонымен қатар, АҚЖ құру іс жүзінде болашақтағы белгісіз оқиғалармен байланысты, сондықтан әрқашан, ең алдымен, жұмыс нәтижесінде пайда болатын белгісіздік элементтерін қамтиды. АҚЖ жобалау кезеңі бастапқыда айтарлықтай белгісіздікпен қатар жүреді. Жоба өскен сайын оның деңгейі

төмендейді, бірақ ешқашан АҚЖ тиімділігі детерминистикалық көрсеткіштермен жеткілікті түрде көрсетіліп, сипатталмайды. Тестілеу, сертификаттау немесе лицензиялау процедуралары АҚЖ немесе оның жекелеген элементтерінің қасиеттерінің белгісіздігін толығымен жоя алмайды және шабуылдардың кездейсоқ сипатын ескермейді. Сондықтан, ықтималдығы, мысалы, белгілі бір шарттар жиынтығында белгілі бір АҚЖ мүмкіндіктерін сипаттау, операция мақсатына қол жеткізу немесе тапсырманы жүйелік орындау, АҚЖ сапасының объективті сипаттамасы, кездейсоқ факторлардың нақты әсері жағдайында қауіпсіздіктің қажетті деңгейіне жетуге бейімделу дәрежесі бола алады. Бұл ықтималдылық, сонымен қатар, АҚЖ тиімділігін бағалау үшін көрсеткіштер мен өлшемдер жиынтығы үшін негіз ретінде қабылдануы керек. Бұл жағдайда бағалау критерийлері жарамдылық және оңтайлылық ұғымдары болып табылады. Жарамдылық дегеніміз АҚЖ үшін белгіленген барлық талаптардың орындалуы, ал оңтайлыдық - бұл жүйенің басқа қасиеттеріне шектеулер мен шарттарды ескере отырып, төтенше мәннің сипаттамаларының біріне қол жеткізу. Нақты критерийді таңдағанда оны АҚЖ мақсатымен үйлестіру қажет [14].

Әдетте жүйені синтездеу кезінде АҚЖ әртүрлі құрылымдарын салыстыру кезінде мультикритерия мәселесі туындайды. Мәселеде қарастырылған индикаторлардың арасында бөлу функциясының ықтималды-уақыттық сипатына ие көрсеткіштер де бар. Атап айтқанда, бұған біраз уақыттан кейін ақпаратты қорғау жүйесін жеңу ықтималдығы кіреді [14].

Осылайша, АҚЖ жұмысының тиімділігін бағалау үшін ықтималды әдістер қолданылады, соған сәйкес АҚЖ-нің кепілдік деңгейлері көрсеткіштердің тиісті бағалауларының сенімділік деңгейіне айналады. Компаниядағы қауіпсіздік кепілдігінің оңтайлы деңгейін бағалау көбіне алдын-ала келтірілген залалға байланысты болады. Тәуекелдің сандық бағасын алу үшін зақымданудың кездейсоқ шамаларының таралуын білу қажет. Көптеген жағдайларда мұндай бағалауларды, мысалы, модельдеу модельдеу немесе АҚЖ белсенді аудитінің нәтижелері бойынша алуға болады [14].

Экономиканың әртүрлі салаларындағы инвестициялардың экономикалық тиімділігін есептеудің бірнеше әдістері бар - өндіріс, сауда, қаржы қызметі, соған қарамастан, қауіпсіздік жүйелерін енгізудегі инвестициялардың тиімділігі өзіндік ерекшеліктерге ие, яғни бұл сала пайда табу үшін емес, құндылығын төмендету үшін құрылды. өрт немесе қызметкерлердің деректерді алып тастауы сияқты қолайсыз жағдайлардың туындау ықтималдығын төмендетеді [15, 16]. Тәуекел кәсіпорынның кез-келген экономикалық қызметіне тән, ол адамдар қабылдаған шешімдердің оң нәтижесіне әсер ететін көптеген жағдайлар мен факторлармен байланысты. Ақпаратты басқару кезінде шаруашылық субъектісінің басшылығы қызмет саласына байланысты белгілі бір кәсіпорында туындайтын тәуекелдердің түрлерін ескеруі керек.

Негізгі материалдар, жабдықтар, бұйымдар және қызметкерлерді оқыту шығындары 5.1 кестеде көрсетілген.

5.1 кесте − АҚЖ енгізу құны, көздерден алынған шығындар [17, 18]

№	Аты	Саны	Құны теңгемен
Құрылғы:			
1	IPS	1	800 000
2	Монтаждық жинақ	1	40 000
Бағдарламалық жасақтама:			
3	БЖ IPS	1	100 000
4	БЖ лог-файлдарды жинау	1	100 000
Техникалық көмек			
5	ТК IPS	1	120 000
6	ТК лог-файлдарды жинау	1	100 000
7	Қызметкерлерді оқыту	2	100 000
8	Қызметкерлер жалақысы	2	4 800 000
9	Құрылғыларды амортизациялау	1	160 000
	Барлығы		6 320 000

Сонымен, ақпараттың қауіпсіздігін қамтамасыз ету жүйесін енгізу бағасы 6,320,000 теңгені құрайды.

Қауіпсіздік жүйесін құруға жұмсалған шығындарды бір реттік шығындар мен пайдалану шығындарының сомасы ретінде көрсетуге болады [19, б.554] және (17) формула бойынша есептеледі.

$$З_{общ} = З_{т} + З_{ед}, \tag{5.1}$$

мұндағы:

$З_{общ}$ – жалпы шығындар (ағымдағы шығындар және бір жолғы инвестициялар) = 6,320,000 теңге;

$З_{т}$ – ағымдағы шығындар = 5 160 000 тг.;

$З_{ед}$ – бір жолғы шығындар = 1 160 000 теңге.;

Бір жолғы шығындар - бұл (18) формулаға сәйкес есептелетін жабдықты сатып алуға, оны орнатуға, қызметкерлерді оқытуға және нормативтік құжаттаманы жасауға шығындар [6, 655 б.].

$$З_{ед} = З_{пр} + З_{м} + З_{об} + З_{д}, \tag{5.2}$$

мұндағы:

$З_{ед}$ – бір жолғы шығындар = 1 160 000 теңге;

$З_{пр}$ – жабдықты сатып алу құны = 800 000 теңге;

$З_м$ – орнату құны = 40 000 теңге;

$З_{об}$ – қызметкерлерді оқытуға шығындар = 100 000 теңге;

$З_д$ – құжаттаманы жасауға шығындар

$З_д = 120000 + 100000 = 220000$ тг.

Ағымдағы шығындар күзет персоналының жалақысынан, жабдықтардың тозуынан және үстеме шығындардан тұрады [19, б.555] және (19) формула бойынша есептеледі.

$$З_т = З_{зп} + З_{ам} + З_н, \quad (5.3)$$

мұндағы:

$З_т$ – ағымдағы шығындар = 5 160 000 тг.;

$З_{зп}$ – жұмысшылардың жалақысына шығындар = 4 800 000 теңге.;

$З_{ам}$ – жабдықтардың амортизациялануына кететін шығын.;

$НАО = 1/60 * 100\% = 0{,}1667 * 12 = 20\%$

$З_{ам} = (800000 * 20\%)/100 = 160000$ тг.;

$З_н$ – есептік шығындар.;

$З_н = 100000 + 100000 = 200000$ тг.

Енді біз кәсіпорынның кірістілік көрсеткіштерін деректерді қорғаудың ұсынылған құралдарының шығындарымен салыстырамыз. Егер бірінші мән екінші көрсеткіштен жоғары болса, онда барлық мақсаттарға қол жеткізіледі және қажеттіліктер қанағаттандырылады. Егер жағдай керісінше болса, онда экономикалық нәтиже болмайды және компания шығынға ұшырайды.

5.2 Ықтимал шығындар көрсеткіштерін есептеу

ROSI Коэффициенті. Құқық қорғау құралдары тікелей кіріс алу құралы болып табылмайды. Сондықтан, қауіпсіздік жүйелерін бағалау кезінде олар алынған ақша туралы емес, ықтимал шығындардың алдын-алу туралы айтады (шығындар азаяды - бұл нақты пайда). «Қауіпсіздікке инвестициялар қайтарымы» (ROSI) терминін алғаш рет 2002 жылы IT қауіпсіздік сарапшылары жасаған.

Қауіпсіздік шығындарының негіздемесі әдеттегідей, ақпаратты қорғаудың корпоративті жүйесіне инвестиция салмай-ақ, компания айтарлықтай артықшылықтарға ие болатындығын дәлелдеді. АҚ шығындарының негіздемесі келесі мәлімдемелерді қамтыды:

- қауіпсіздік шығындары бизнесті жүргізуге кететін шығындардың бөлігі болып табылады;
- қауіпсіздік шығындары сақтандыру шығындарымен байланысты;
- компания электронды ақша ағындарын қорғаудың белгілі бір деңгейін қамтамасыз етусіз электронды сауда-саттықпен айналыса алмайды;
- қауіпсіздік - тәуекелдерді басқарудың бір аспектісі;

- егер тұтынушы қауіпсіздіктің минималды стандарттарын орындаудан бас тартса, компанияны сотқа жүгінуге құқылы (мысалы, тұтынушының құпия ақпаратын қорғау);

- қауіпсіздікке инвестиция салғысы келмеу дегеніміз - IT дамуының жалпы тенденцияларын ұстанбау.

Осындай дәлелдер келтіргеннен кейін, компанияның ақпараттық қауіпсіздігіне шығындар қажет екендігіне ешкім күмән келтірмейді, бірақ ақпаратты қорғаудың корпоративтік жүйесіне инвестицияларды қаржылық негіздеу үшін сандық есептеулер қажет.

Ақпаратты қорғауға қажетті инвестицияны есептеудің бірнеше әдістері бар.

Күтілетін шығын әдісі. Бұл тәсіл қауіпсіздік саясатының бұзылуынан болатын шығындар есептелетініне және осы шығындар бұзушылықтардың алдын алуға бағытталған қауіпсіздікке салынған инвестициялармен салыстырылатындығына негізделген. Күтілетін шығын әдісі ұйымдардың эмпирикалық тәжірибесіне және интрузиялар туралы ақпаратқа, вирустардан болатын шығындар туралы, сервистік шабуылдар туралы және т.б.

Мысалы, коммерциялық ұйымдардың қауіпсіздігін бұзу келесі қаржылық шығындарға әкеледі:

- электронды сауданы жүргізу кезінде, тоқтап қалумен және желілік жабдықтың істен шығумен байланысты шығындар;

- компанияның беделіне және беделіне нұқсан келтіру;

- IT қызметкерлерінің үстеме жұмысы үшін және / немесе корпоративтік ақпараттық жүйені қалпына келтірумен айналысқан мердігерлерге жұмыс үшін ақы төлеу;

- деректерді қалпына келтіруді, жөндеу жұмыстарын жүргізген және заңгерлік көмек көрсеткен сыртқы мамандардың кеңесіне ақы төлеу;

- виртуалды шабуылдардан келтірілген зиянды қалпына келтіру үшін төлем;

- виртуалды қылмыстар және қауіпсіздік саясатын бұзу туралы талап арыз беру кезіндегі сот шығындары.

Күтілетін шығынды «азайту» үшін компания қауіпсіздікке қаржы бөлуі керек: брандмауэр, шабуылдардың алдын-алу үшін жүйені анықтау жүйелері, вирустардың әр түрлі формаларын анықтайтын антивирустар.

Егер компания ақпараттық қауіпсіздік жүйесін орнатуды ұйғарса, онда оның мәні келесідей жинақталады:

- бір реттік шығындар. Бұл әдетте жабдықтың құны, сонымен қатар ақпараттық қауіпсіздік жүйелерін енгізу;

- қайталанатын шығындар. Техникалық қолдау және қолдау, IT қызметкерлерінің жалақысы, антивирустық лицензияларды жаңарту және басқа бағдарламалық қамтамасыз ету сияқты параметрлер бар.

Ақпараттық қауіпсіздік жүйесін енгізудің әсерін анықтау үшін күтілетін шығындар индикаторын есептеу керек (Жыл сайынғы шығындар күтуі - ALE). Мамандардың пікірінше, дұрыс орнатылған және конфигурацияланған

қорғаныс жүйесі қауіпсіздік саясатын бұзудан болатын шығындарды болдырмауға немесе азайтуға 85% тиімділік береді. Демек, қаржылық пайда компания (5.5) формуласына сәйкес АҚ жүйесін [20] енгізу кезінде алатын жылдық үнемдеу арқылы қамтамасыз етіледі.

$$AS = ALE \cdot E - AC, \qquad (5.4)$$

мұндағы:

AS – жылдық жинақ (Annual Saving),

ALE – күтілетін шығын көрсеткіші (Annualised Loss Expectancy),

E – қорғау жүйесінің тиімділігі (85% арасында),

AC – жылдық қауіпсіздік шығындары (Annual Cost).

Қауіпсіздік атрибуттарын бағалау әдісі (SAEM) Carnegie Melon University-де әзірленді және АЖ жүйесін енгізудің артықшылықтарын бағалаудың өзіндік құнына негізделген нәтижелерді алу үшін әртүрлі АЖ жүйелерінің архитектураларын салыстыруға негізделген. SAEM тәуекел мен сыйақыны сандық бағалауға сүйенеді, оның барысында аналитик немесе тергеуші бастапқы деректерді алу үшін IT және қауіпсіздік менеджерлерімен құрылымдалған сұхбат жүргізеді. SAEM әдістемесі оқиғаның ықтималдығын үйлестіруден және қоршаған ортаға әсерді салыстырудан тұрады, әр түрлі ақпараттық қауіпсіздік жобаларын салыстырмалы шығындарға қоршаған ортаға көп әсер ететін жобаларды ұсынады.

Бұл әдістің кемшілігі, көбінесе қауіпсіздік тиімділікті бағалауға қатысатын менеджерлерді түсінбейді, ал ақпараттық қауіпсіздік бойынша мамандар технологияның пайдасы туралы сирек дәл мәліметтерге ие болады, сондықтан сіз тәжірибе мен түйсігіге сүйеніп, соларға сүйене отырып шешім қабылдайсыз.Методика Return on Investment for Security

Күтілетін шығын әдісін қауіптер мен тәуекелдерді бағалау кестесімен біріктіре отырып, біз кіріс жағын есептейміз.

Бірінші қадам - TRA кестесін құру. Кішігірім дағдарыс жасап, ақпараттық қауіпсіздікті қамтамасыз ету үшін қарсы шараларға қысқаша сипаттама берейік.

Қауіпсіздікке қарсы шаралар келесі нәтижелерге қол жеткізуге бағытталған: егер инциденттің ықтималдығын төмендету және / немесе егер ол әлі де болса орын алса, оның салдарын азайту.

Ықтималдылықты төмендететін шаралар профилактикалық деп аталады, ал әсерін төмендететін шаралар емдік деп аталады. Апаттың ықтималдығы «шамалы» -дан «төтенше» деңгейге дейін жеті деңгейде сипатталсын. Бұл деңгейлерді келесі кестеде анықтаймыз [20] (5.3 кестені қараңыз).

Қауіпсіздік саясатын бұзудың салдары сонымен қатар «маңызды емес» деңгейден «маңызды» деңгейге дейінгі алты деңгеймен сипатталады және Gartner Group сарапшылары анықтаған бұзушылықтарды жою жағдайындағы шығындарға сәйкес келеді (5.2 кестені қараңыз).

Ошибка! Текст указанного стиля в документе отсутствует..1 кесте – Қорғаныс түрлері

Қорғау түрі	Мысал
Профилактикалық	1. Стандарты, процедуры, должностные инструкции
	2. Аудит системы безопасности
	3. Желілік экрандар
	4. Интрузияны анықтау жүйелері
	5. Антивирустар
	6. Шифрлау құралдары
	7. Мұрағаттау
Емдік	Күту режимдері
Екі түрге де қатысты	1. Бизнестің үздіксіздігін жоспарлау / бизнесті қалпына келтіруді жоспарлау
	2. Оқыту

5.2.2 ROSI есептеулері. Енді біз ALE индикаторын қауіптің ықтималдығын, бұзушылықтың ауырлығын және оқиғалардың жиілігін салыстыратын TRA кестесінің формуласын қолдана отырып есептейміз (5.3 кестені қараңыз). ALE индикаторын [20] формула бойынша есептейміз:

$$ALE = f \cdot L, \tag{5.5}$$

мұндағы:

f – ықтимал қауіптің пайда болу жиілігі, оның деңгейі ықтималдылық негізінде анықталады [20] (5.3 кестені қараңыз);

L – теңгедегі шығын мөлшері, ол бұзушылықтың ауырлығына қарай анықталады [20] (5.4 кестені қараңыз).

Ошибка! Текст указанного стиля в документе отсутствует..2 кесте – Қауіптердің ықтималдығы және оқиғалардың жиілігі [20]

Ықтималдық деңгейі	Сипаттамасы	Жиілік
Болмашы	Болуы екіталай	0,05
Өте төмен	Оқиға бес жылда екі-үш рет өтеді.	0,6
Төмен	Оқиға жылына бір реттен сирек емес өтеді	1,0
Орташа	Оқиға алты айда бір реттен сирек немесе алты айда бір рет болады	2,0
Жоғары	Оқиға айына кемінде немесе айына бір рет болады	12,0
Өте жоғары	Оқиға айына бірнеше рет өтеді	24,0
Экстремальді	Оқиға күніне бірнеше рет өтеді	365,0

Ошибка! Текст указанного стиля в документе отсутствует..3 кесте – Ауырлық пен шығын рубльден аударылған. тг. 28.05.20 жылғы ҰБ бағамы бойынша 5.9 тг

Бұзушылықтың ауырлығы	Сипаттамасы	Шығындар, тг
Болмашы (1)	Саналы түрде қауіп төнген жағдайда бұзушылықтың салдары болмайды	0
Төмен (2)	Бұзушылық қаржылық шығындарға алып келмейді, бірақ оқиғаның мән-жайын анықтау аз шығындарды талап етеді.	80 000
Елеулі (3)	Оқиға материалдық және моральдық зиян келтіреді.	500 000
Қауіпті (4)	Беделді, құпия ақпаратты жоғалту. Мәліметтерді қалпына келтіру, зерттеу шығындары	1 500 000
Өте қауіпті (5)	Электрондық және қағаздағы барлық дерлік деректерді қалпына келтіру	4 000 000

Ақпараттық қауіпсіздікке салынған инвестицияларды негіздеудің келесі қадамы инвестициялардың қайтарымдылығын талдау болып табылады. Бастапқыда біз ақпараттық қауіпсіздік жүйесін енгізу шығындарын анықтаймыз.

Қауіпсіздіктің тиісті деңгейін қамтамасыз ету үшін ақпараттық қауіпсіздік жүйесінің келесі элементтерін енгізу қажет: Интернет шлюзін қорғау жүйесі, файлдық серверлер мен жұмыс станциялары үшін антивирустық қорғау жүйесі және электрондық поштаны қорғаудың корпоративтік жүйесі.

Пайдаланылған қорғаныс құралы ретінде шлюздер мен электрондық поштаны қорғаудың, файлдық серверлер мен жұмыс станцияларын қорғаудың екі тәсілі бар шешім таңдалды.

Шешімдер жиынтығын іске асыру шығындары [20] 5.5 кестеде келтірілген.

Ақпараттық технологияларды енгізуге байланысты инвестициялық жобалардың ақталу мерзімі үш жылдан аспауы керек, сондықтан осы жобаны іске асырудың тиімділігін бағалау мерзімі - үш жыл.

Ошибка! Текст указанного стиля в документе отсутствует..4 кесте − Күтілетін шығындар индикаторын есептеу [20]

№	Актив	Ықтимал қауіп	Ықтималдық деңгейі	Дәреже	Жылына жиілік	Шығын, тг	ALE, тг
1	Интернет каналдары	Негізгі инфрақұрылымды бұзу	Болмашы	(5)	0,05	4 000 000	200 000
		Салқындату жүйесінің ақауы	Орташа	(3)	2	500 000	1 000 000
		Ақпараттың құпиялығын бұзу	Төмен	(4)	1	4 000 000	4 000 000
		Құрылғының зақымдалуы	Өте төмен	(4)	0,6	1 500 000	900 000
		инфрақұрылым	Төмен	(3)	1	500 000	500 000
		Инфрақұрылымның дұрыс салынбауы	Өте төмен	(3)	0,6	500 000	300 000
		Желілік инфрақұрылымға шабуыл	Болмашы	(4)	0,05	1 500 000	75 000
2	Электрондық пошта жүйесі	Электрондық поштаға шабуыл	Өте жоғары	(3)	24	500 000	12 000 000
3	Бизнес қосымшасы	Құжатты басып шығару мәселесі	Жоғары	(1)	12	0	0
		Бизнес қосымшалардың сенімділігінің бұзылуы	Төмен	(4)	1	1 500 000	1 500 000
		Корпоративтік құжат айналымы жүйесінің бұзылуы	Төмен	(4)	1	1 500 000	1 500 000
Барлығы						16 000 000	21 975 000

ROI көрсеткіші. Бизнесте инвестициялау кезінде ROI (Return on Investment) түсінігі бар, ол белгілі бір компанияға салынған инвестицияны қайтаруға қанша уақыт кететінін анықтайды. ROI мәнін есептеу үшін (22) [20] формула қолданылады:

$$ROI = \frac{Income - Consumption}{Investments}, \tag{5.7}$$

мұндағы:

Income – есепті кезеңдегі (жылдағы) компанияның кірісі,

Consumtion – есепті кезеңдегі (жылдағы) компания шығындары,

Investments – компанияға салынған инвестициялар.

Бұл алынған ақшаның пайыздық мөлшерлемемен көрсетілген бір бағытта немесе басқа бағытта салынған адамдарға қатынасы. Қатаң түрде, ROI - бұл жобаны іске асыру үшін қажетті инвестициядан түскен пайдадан (немесе экономикалық тиімділік) пайыздық мөлшер. Жақсырақ түсіну үшін мен бірнеше мысал келтіремін [20].

Біз (5.5) формула бойынша есептейміз - жылдық жинақ (Annual saving) (5.6 кестені қараңыз).

Ошибка! Текст указанного стиля в документе отсутствует..5 кесте – Жылдық жинақтарды есептеу

Параметрлер	1-жыл	2-жыл	3-жыл
Қорғаныс жүйесінің тиімділігі	85%	87%	90%
Күтілетін шығын мөлшері	21 975 000	21 975 000	21 975 000
Жыл сайынғы қауіпсіздік шығындары	6 320 000	5 020 000	5 020 000
Жылдық жинақ	12 358 750	13 658 750	13 658 750

(22) формула бойынша есептеледі (ROI):

$$ROI = \frac{12358750 - 6320000}{6320000} * 100\% = 95{,}549\%.$$

Инвестициялардың қайтарымы 95,549% құрайды.

Жобаның өтелу мерзімін есептеу. Абсолютті экономикалық тиімділік тең болады [21]:

$$E = \frac{12358750}{6320000} = 1{,}955.$$

Жобаның өтелудің есептік мерзімі абсолютті экономикалық тиімділіктің қайтарымы ретінде анықталады [21]:

$$T = \frac{1}{E} \cdot 12 ай = \frac{1}{1,955} \cdot 12 ай = 6 \text{ ай және 5 күн.}$$

Жобаның ақталу мерзімі - 6 ай және 5 күн.

Қорытынды

Бұл дипломдық жұмыстың негізгі мақсаты ретінде алынған байланыс желілеріндегі ақпараттық қорғау әдістері мен құралдарының бірнеше түрі келтірілді.

Cisco компаниясы ұсынған Packet Tracer желіні жоспарлауға арналған симулятормен байланыс желілерде жоғары ақпарат қауіпсіздігіне кол жеткізуге болатын бірнеше әдістер көрсетілді және сол бағдарламалармен жұмыс жасайтын аппараттар тізімі жасалып, жұмысымызға лайықты ақпараттық қауіпсіздікті қамтамасыздықты ұсына алатын IPS жүйесі таңдалынып алынды.

Тіршілік қауіпсіздігі бөлімінде еңбек жағдайларын егжей-тегжейлі зерттеу жүргізілді. Кәсіпорынның жұмысшы құрамы өздерінің еңбек қызметі барысында ұшырайтын негізгі қауіпті және зиянды факторлар анықталды, сонымен қатар жабдықтар мен жұмыс орындарын оператор бөлмесінде орналастыру жоспары келтірілді.

Сервер бөлмесіндегі жабдықтардың қалыпты жұмысы үшін олар ГОСТ талаптарына сәкес орналастырылынды және сәйкес микроклимат орнатылды. Қажетті микроклимат қалпын сақтау үшін AM SDAC 0251A дәлме-дәл кондиционері таңдап алынды. Өрттен қорғауды қамтамасыз ету үшін сервер бөлмесі автоматты өрт дабылымен жабдықтанды , өрт сөндіргіші ретінде Novec™ 1230 қолданылды. Электр қауіпсіздігі ескеріліп, жерге тұйықталу есептелінді.

Экономикалық бөлімде ақпараттық қауіпсіздікті қамтамасыз ету құны есептелінді. Жобаның ақталу мерзімі 6 ай және 5 күнді қамтыды.

Қорытындылай келгенде байланыс желілердегі қауіпсіздікті қамтамасыз ету әдістері өте көп және әрқайсысының өз тұрақты әрі топтама тұстары бар екені анықталды. Өткізу жылдамдығы күннен күнге артып келе жатқан жаңа технологиялар арқылы ақпарат алмасу жұмыс бабын оңайлатқанымен, оларды қорғау қиындап бара жатқаны да бар. Сол себепті технологияның даму барысымен бірге сол технологияның ақпараттық көздерінің қауіпсіздігіне қойылатын талаптардың да арта түсетіні хақ. Ал бұл дипломдық жұмыста көрсетілген технологиялар жиынын өзінара байланыстырып қолдана білсек жоғары деңгейдегі ақпараттық қауіпсіздікті алуға болады.

Әдебиеттер тізімі

1 N. Fisk. Malware Incidents // Encyclopedia of Cybercrime / Samuel C. McQuade, III. — London : Greenwood Press, 2009. — P. 124. — ISBN 978-0-313-33974-5

2 Anderson, James P., "Computer Security Threat Monitoring and Surveillance, " Washing, PA, James P. Anderson Co., 1980

3 Dowell, Cheri, and Ramstedt, Paul, "The ComputerWatch Data Reduction Tool, " Proceedings of the 13th National Computer Security Conference, Washington, D.C., 1990

4 EOTP – Static Key Transfer. Defuse.ca (2012-07-13). Retrieved on 2012-12-21.

5 Евгений Зобнин. Журнал "Хакер", Устоять любой ценой. Методы борьбы с DoS/DDoS-атаками. — 2009.

6 Eric Stewart. CCNA Security Exam Cram (Exam IINS 640-553) (англ.). — Pearson Education (англ.)русск., 2008. — P. 46—. — ISBN 978-0-7686-8683-8.

7 Newman, Robert (2009-06-23). Computer Security: Protecting Digital Resources. Jones & Bartlett Learning. ISBN 9780763759940

8 ГОСТ 12.2.032-78. «ССБТ. Рабочее место при выполнении работ сидя. Общие эргономические требования»

9 СанПиН 2.2.2/2.4.1340-03 - Требования к помещениям для работы с ПЭВМ

10 ГОСТ 12.1.003-83 - «Система стандартов безопасности труда Шум. Общие требования безопасности»

11 СН 512-78 - Технические требования к зданиям и помещениям для установки средств вычислительной техники.

12 ANSI/TIA/EIA-569-A – «Стандарт телекоммуникационных трасс и пространств коммерческих зданий»

13 Ж.С. Абдимуратов. Охрана труда. Методические указания к выполнению расчетно-графических работ для студентов - бакалавров специальности 5В071800- «Электроэнергетика» - Алматы: АУЭС, 2013 - 22с.

14 Оценка эффективности мероприятий информационной безопасности в условиях неопределенности // Bijournal.hse.ru: Научный журнал «бизнес-информатика». URL: https://bijournal.hse.ru/data/2015/05/28/1096865620/5.pdf (дата обращения: 28.05.2019).

15 Орлова, Е.Р. Инвестиции: учеб. Пособие / Е.Р. Орлова. М.: Омега-Л, 2016, 156 стр.

16 Информационно-аналитический журнал «Рубеж» // [Электронный ресурс] / URL: https://ru-bezh.ru/ (дата обращения: 04.05.2019).

17 Брандмауэр нового поколения // Checkpoint.com: Software technologies ltd. URL: https://www.checkpoint.com/ru/products/next-generation-firewall/ (дата обращения: 28.05.2019).

18 Splunk Enterprise // Splunk.com: analyzing machine-generated big data. URL: https://www.splunk.com/en_us/software/splunk-enterprise.html (дата обращения: 28.05.2019).

19 Галиуллина, Р.А. Разработка методики расчета экономического эффекта от внедрения системы безопасности // Р.А. Галиуллина, А.В. Ларина, А.П. Орлова. Новосибирск: СибАк, 2016. 857 с.

20 Окупаемость ИБ-систем. Какую прибыль может принести система ИБ // Samag.ru: Системный администратор. URL: http://samag.ru/blog/art/No_number/16 (дата обращения: 27.05.2019).

21 Методические указания для экономической части выпускной работы составители: Базылов К. Б.,Алибаева С. А.,Бабич А. А.- АИЭС.- 2008г.