МАТЕРИАЛЫ

V - МЕЖДУНАРОДНОЙ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ «ИНФОРМАТИКА И ПРИКЛАДНАЯ МАТЕМАТИКА», ИНСТИТУТА ИНФОРМАЦИОННЫХ И ВЫЧИСЛИТЕЛЬНЫХ ТЕХНОЛОГИЙ

29 сентября - 01 октября 2020 года

Институт информационных и вычислительных технологий МОН РК

Казахский Национальный Университет имени аль-Фараби

Университет Туран

Люблинский технический университет, Польша

«Ғылым ордасы»

МАТЕРИАЛЫ

V международной научно-практической конференции "Информатика и прикладная математика", 29 сентября - 1 октября 2020, Алматы, Казахстан

Алматы 2020

УДК 378 (063)
ББК 74.58
И74

Главный редактор:
Калимолдаев М.Н. - генеральный директор ИИВТ, академик НАН РК, доктор физико-математических наук, профессор

Ответственные редакторы:
Мамырбаев О.Ж. - заместитель генерального директора ИИВТ, доктор PhD
Калижанова А.У. - заместитель генерального директора ИИВТ, кандидат физико-математических наук
Юничева Н.Р. - ученый секретарь ИИВТ МОН РК, кандидат технических наук, доцент

И 74 **Информатика и прикладная математика:** Мат. V Межд. науч. конф. (29 сентября -1 октября 2020 г.). Алматы, 2020. – с. 435

ISBN 978-601-332-384-8

В сборнике опубликованы доклады, представленные по 4 секциям от Республики Казахстан, Российской Федерации, США, Латвии, Польши, Республики Беларусь, Украины, Азербайджана, Узбекистана, Японии, Кореи, Ирана, Португалии, Испании, Великобритании, Греции, Кыргызской Республики и других.

Рассмотрены актуальные вопросы в области математики, информатики и управления: математического моделирования сложных систем и бизнес-процессов, исследования и разработки защищенных и интеллектуальных информационных и телекоммуникационных технологий, математической теории управления, технологий искусственного интеллекта.

Материалы сборника предназначены для научных работников, докторантов и магистрантов, а также студентов старших курсов.

УДК 378 (063)
ББК 74.58

ISBN 978-601-332-384-8

© Институт информационных и вычислительных технологий МОН РК, 2020

Возможность дальнейшего развития предложенной системы двухфакторной аутентификации заключается в расширении компонентов (например, используется уже такая терминология, как «Композитная аутентификация»), применении отечественных криптографических алгоритмов, разработке дополнительных инструментов и оптимизации решений с целью повышения производительности.

Литература

1 Нысанбаева С.Е., Усатова О. А. «Способы обеспечения безопасности информации в базах данных»// Вестник КазНИТУ им. Сатпаева.– Алматы, 2018. – № 2. – С. 66–70.

2 Нысанбаева С.Е., Усатова О.А. «Двухфакторная аутентификация в автоматизированной системе управления»// III Междунар. науч. конф. «Информатика и прикладная математика». – Алматы, 2018. – С. 239–242.

3 S. Nyssanbayeva, W. Wojcik, O. Ussatova «Algorithm for generating temporary password based on the two–factor authentication model»// Przegląd Elektrotechniczny. – Polan, 2019. –№ 5. – P. 101–106.

4 Olga Ussatova, Saule Nyssanbayeva «Generators of one-time two-factor authentication passwords»// Informatyka, Automatyka, Pomiary w Gospodarcei Ochronie Środowiska. – Poland, 2019. № 2. – P. 60–64.

5 O. Ussatova, S. Nyssanbayeva, W. Wojcik «Development of an authentication model based on the second factor in an automated control system»// Вестник КБТУ. – Алматы, 2019. –Т.16. – С.115–118.

6 O. Ussatova, S. Nyssanbayeva, W. Wojcik «Two-factor authentication algorithm implementation with additional security parameter based on mobile application »// International Conference on Wireless Communication, Network and Multimedia Engineering (WCNME2019). –Guilin, China, 2019. – Vol. 89. – P. 84–86.

7 Begimbayeva Yenlik, Ussatova Olga, Biyashev Rustem, Nyssanbayeva Saule «Development of an automated system model of information protection in the cross-border exchange»// Cogent Engineering Journal. – 2020. DOI: 10.1080/ 23311 916. 2020.1724597. –P. 1–13.

8 O. Ussatova, S. Nyssanbayeva, W. Wojci. « Software implementation of two-factor authentication to ensure security when accessing an information system» // Вестник КазНУ им.аль-Фараби. –Алматы,2019. – С.87–95.

9 Усатова О.А. «Клиент-серверная система защиты информации на основе двухфакторной аутентификации»// междунар. науч.– практ. конф. «Актуальные проблемы информационной безопасности в Казахстане». – Алматы, 2020. – С. 243–248.

ЖЕЛІЛІК ТОПОЛОГИЯНЫҢ ҚАУІПСІЗДІК МОДЕЛІ МЕН ӘДІСТЕРІН ӘЗІРЛЕУ

Ордабаева Г.К.
e-mail: gulzi200988@mail.ru
Әл-Фараби атындағы Қазақ ұлттық университеті, PhD докторант, Қазақстан

***Аннотация**: Бүгінгі таңда, ақпараттық жүйелерге қауіп төндіретін модельдерді құрудың көптеген тәсілдері белгілі. Бұл тәсілдер нормативтік актілерде және стандарттарда, әртүрлі компаниялардың құжаттарында және ғылыми зерттеулерде сипатталған.*

Мақалада қауіптерді анықтауда және қауіпсіздікті бағалауда қолданылатын компьютерлік желілердің модельдерін құру тәсілдері мен әдістері қарастырылды.

Кіріспе

Ақпараттық технологиялардың қарқынды дамуы үшін желі топологиясының сенімділігін арттыру өзекті міндеттердің бірі. Мұндай мәселелерді шешу үшін қолданыстағы желілік архитектураларды әзірлеу, желі арқылы ақпараттық ресурстарды тарату кезіндегі қауіптерді зерттеу қажеттігі туындайды.

Компьютерлік желілер модельдері қарастыратын бөліміне байланысты келесі топтарға бөлінеді [1]:

- тұжырымдамалық (концептуальдық) модельдер [2, 3];
- функционалды модельдер [4];
- математикалық модельдер [5].

Тұжырымдамалық модельдер сипатталған жүйенің құрылымын, оның элементтерінің қасиеттерін, бейресми тілде модельдеу мақсаттарына жету үшін маңызды себеп-салдарлық байланыстарды анықтайды. Бұл үшін әдетте графиктер, кестелер, диаграммалар және т.б. қолданылады.

Сипаттамалық графикалық модельдер өзара әрекеттесетін және өзара байланысты блоктар жиынтығын қолдана отырып, функционалды модельдер ұйымның жұмыс істеуі аясында қалай жасалатынын көрсетеді.

Математикалық модельдер формулалар, графиктер, мысалдар және т. б. арқылы сипатталады, сонымен қатар, әлеуметтік, техникалық және жаратылыстану ғылымдарында, әртүрлі дизайн мәселелерін шешуде қолданылады [6].

Негізгі бөлім

Ашық жүйелердің өзара байланысының (Open System Interconnection, OSI) Халықаралық стандарты бойынша компьютерлік желі жеті деңгейге бөлінеді: қолданбалы, көрсету, сеанстық, транспорттық, желілік, арналық және физикалық. OSI моделінің физикалық, арналық және желілік деңгейлеріне проекцияда таратылған есептеу жүйесі объектілерінің өзара әрекеттесу моделі [7] жұмыста сипатталған. Нақты желілік шарттарға, қызметтер үстемділігіне және басқа факторларға байланысты жіберуші мен қабылдаушы компьютерлер арасындағы бағыт анықталады. Таратылған есептеу жүйелері моделінің негізгі міндеті берілген кіріс параметрлері арасында байланыс орнату.

Проекциядағы OSI физикалық деңгейінің моделі таратылған есептеу жүйесінің объектілері арасындағы физикалық байланысты анықтайды. OSI арналық деңгейіне проекциядағы желілік адаптерлердің аппараттық адрестері деңгейіндегі объектілердің өзара әрекеттесуін орнатады. Проекциядағы OSI объектілерінің желілік деңгейге байланысы логикалық адрестер деңгейінде анықталады.

OSI моделінің физикалық деңгейінде желілік кабель арқылы жіберілетін әрбір биттің ұзақтығы және оның сәйкес электрлік немесе оптикалық импульсқа көшірілуі анықталады. OSI моделінің арналық деңгейіне проекциядағы желілік адаптерлердің аппараттық адрестері деңгейіндегі объектілердің өзара әрекеттесуін орнатады. Желілік деңгейге проекцияда OSI моделі объектілерінің байланысы логикалық адрестер деңгейінде анықталады.

Жұмыста әмбебап *KS* желісі енгізіледі, ол физикалық немесе арналық OSI деңгейінің байланыс сызығы ретінде түсініледі, өйткені, физикалық және арналық деңгейлердің проекциядағы моделдерінде айырмашылық жоқ. Физикалық деңгейдегі объектілер - хост немесе роутердің желілік адаптері, арналық деңгейдегі объектілер – желілік адаптердің аппараттық адресі.

Берілген таратылған есептеу жүйесінде *N* өзара байланысқан *KS* (физикалық және арналық деңгейдегі байланыс желілері) және *LS* (желілік деңгейдегі байланыс желілері) объектілер мен роутерлерді қамтиды, яғни:

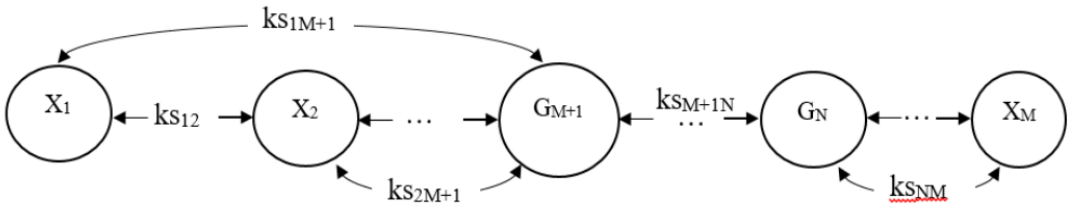
$X = \{x_i | i=1..M\}$ – хостар жиыны,
мұнда $i=1..M$ –хостар саны.

$G=\{g_i | j=M+1..N\}$ –роутерлер жиыны,
мұнда $j=M+1..N$ –роутерлер саны.

Физикалық немесе арналық деңгейінде әр хост тек бір ғана жақын роутермен байланысады. Барлық нысандар *K* объектісін *L* объектісімен байланыстыратын қос бағытты байланыс желілері ks_{KL} арқылы өзара әрекеттеседі.

$KS=\{ks_{KL} | k=1..N, L=1..N\}$,
мұнда *KS* - OSI моделінің физикалық немесе арналық деңгейіндегі байланыс желілерінің жиынтығы.

Проекциядағы ақпараттық жүйенің OSI моделінің арналық немесе физикалық деңгейінің граф моделі 1- суретте көрсетілген.

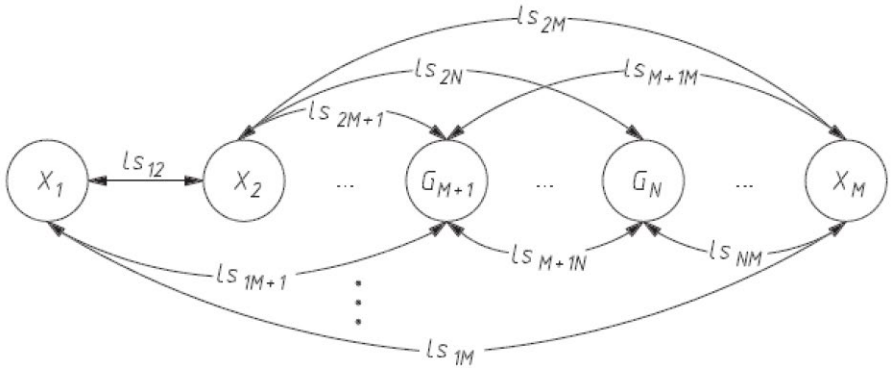


1- сурет. Проекциядағы OSI моделінің физикалық немесе арналық деңгейінің граф моделі

Желілік деңгейде әр объект басқа объектімен (кез - келгенімен) бір-екі бағытты ls_{KL} байланыс желісінің көмегімен өзара әрекеттесе алады, ол *K* объектісін *L* объектісімен байланыстырады. Бұл деңгейде хосттың немесе маршрутизатордың желілік адресі объект болып табылады.

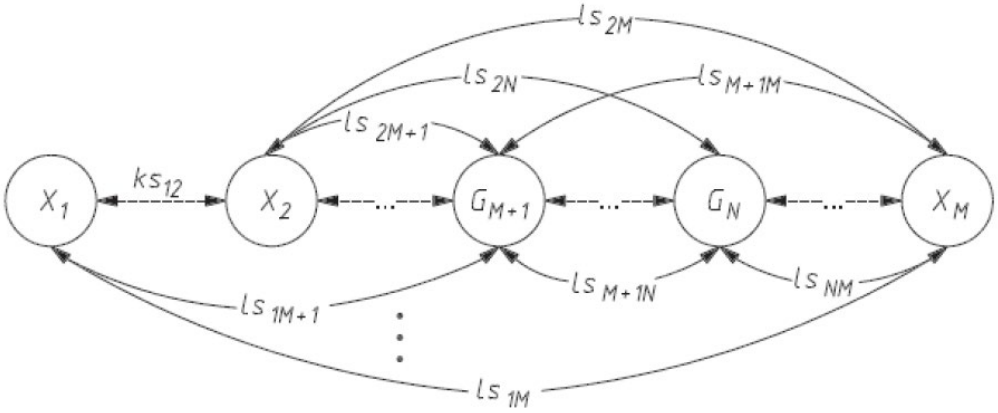
$LS=\{ls_{KL} | k=1..N, L=1..N\}$,
мұнда *LS* – желілік деңгейдегі объектілердің көптеген байланыс сызықтары.

Граф көмегімен ұсынылған проекциядағы ақпараттық жүйенің желілік деңгейдегі моделі 2-суретте көрсетілген.



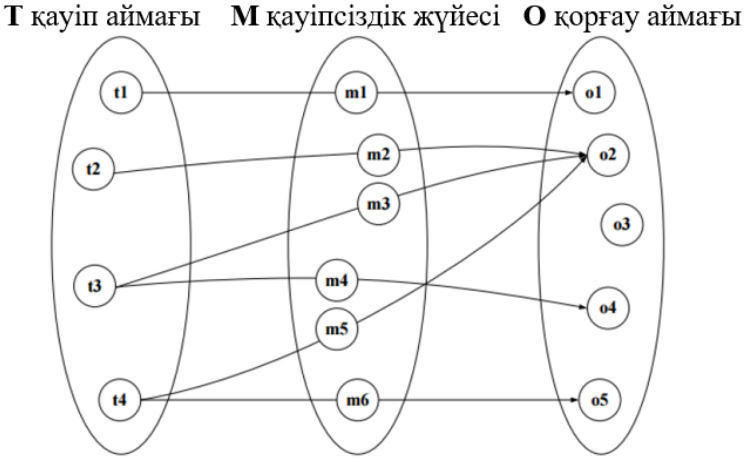
2-сурет. OSI желілік деңгейіне проекциядағы граф моделі

OSI моделінің физикалық және желілік деңгейлеріне проекциядағы объектілердің өзара әрекеттесу моделі 3- суретте көрсетілген.



3-сурет. OSI физикалық және желілік деңгейлеріне проекциядағы граф моделі

Королёва О.Ю., өз жұмысында ақпараттық қауіпсіздік жүйесін сипаттау үшін 4-суретте берілген үш жақты граф моделін қолданған [8]. Қауіп-объект қатынастар жиыны екі жақты графикті {T, O} құрайды. M үшінші жиынын енгізу бағандағы барлық мүмкін беттерді жабады. Нәтижеде -S= {T, M, O} үш жақты граф моделі құрылады.

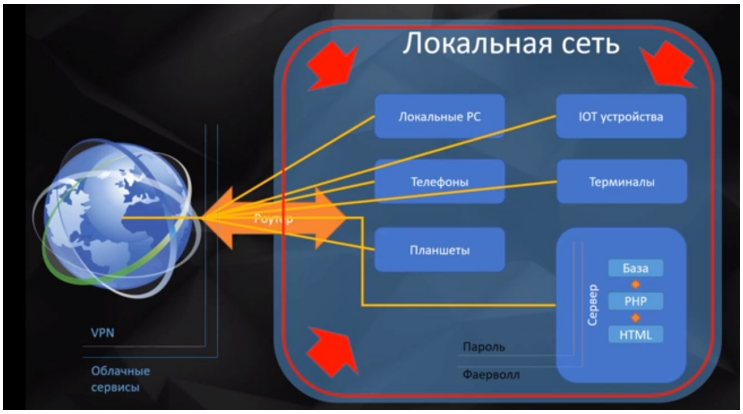


4-сурет. Ақпараттық қауіпсіздікті қамтамасыз ету жүйесінің граф моделі

Ақпараттық қауіпсіздік туралы мәліметтер нормативтік құжаттардан және ақпаратты қорғау мәселелерімен айналысатын компаниялардың зерттеулері мен есептерінен алынады [9, 10].

Бүгінде компьютерлік желінің қауіпсіздігін анықтаудың бірнеше әдістері бар. Қарапайым әдістің бірі ретінде – Nessus Vulnerability Scanner негізінде желінің осалдығын анықтау жолдарын қарастырдық. Желі осалдығын анықтаудың негізгі мақсаты – желіні қорғаудағы әлсіз буынды анықтау [11].

5-суреттегі желі мысалында, роутер арқылы бүкіләлемдік байланысқа шығамыз, сонымен қатар, барлық ішкі құрылғылар өзара ешқандай құпия сөздерсіз (пароль) байланыс жасай алады.

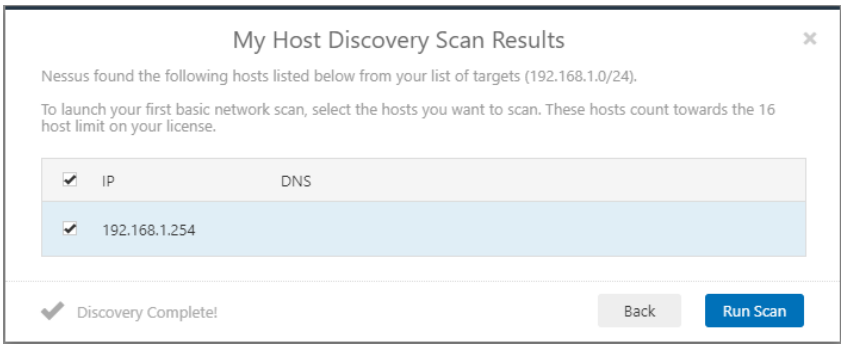


5-сурет. Локальды желі байланысы [12]

Осалдықты анықтаудағы міндеттер:

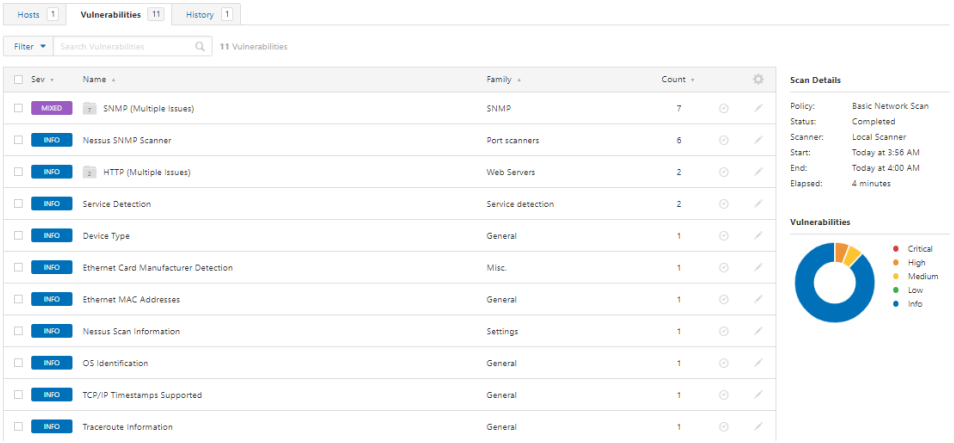
- желілік инфрақұрылымда, бағдарламалық және аппараттық құралдарда, қосымшаларда кездесетін осалдықтарды анықтау;
- анықталған «қауіпсіздік саңылауларының» гипотетикалық сценарийінің салдарын түсіндіру;
- анықталған қатерлермен күресу стратегиясын әзірлеу;
- компанияның қауіпсіздігін жақсарту және қауіпсіздік тәуекелдерін жою бойынша ұсыныстар беру.

Nessus Vulnerability Scanner толықтай орнатылғаннан соң ашылған сұқбаттық терезеде 192.168.1.0/24 IP адресінің барлық ішкі желісін сканерлейміз.



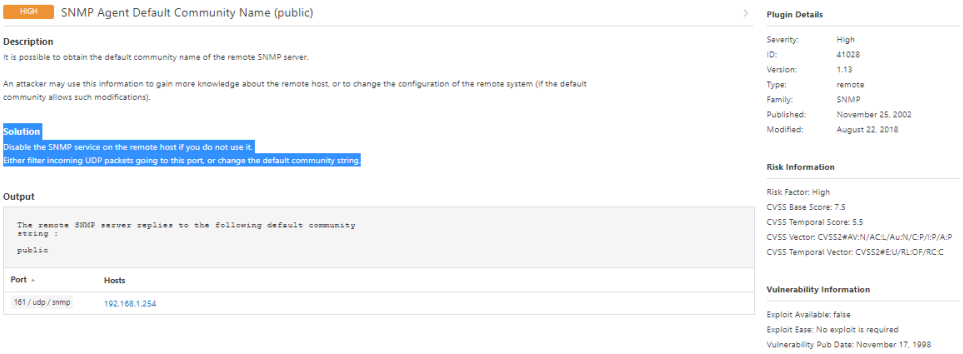
6 – сурет. Ішкі желіні сканерлеу [11]

Сканерлеу нәтижелері бойынша біз IP адрестер тізімін және осы адрестерге байланысты осалдықтарды аламыз. Осалдықтар түрлі түстермен берілген (7-сурет).



7-сурет. Сканерлеу нәтижесінде анықталған осалдықтар

Қажетті осалдықты белгілей отырып толық ақпарат алуға болады және осы есепті қалаған форматта сақтай аламыз. Мысалы, SNMP Agent Default Community Name (public) осалдығына берілген талдау және осалдықты жою жолдары 8 - суретте көрсетілген.



8-сурет. Анықталған осалдыққа талдау

Қорытынды

Мақалада OSI моделінің физикалық, арналық және желілік деңгейіндегі таратылған есептеу жүйесі объектілерінің өзара әрекеттесуін сипаттайтын бағытталған графты қолдана отырып жасалған ақпараттық жүйенің моделі берілген.

Қолданылуы қарапайым Nessus Vulnerability Scanner негізінде желінің осалдығын анықтау әдісі келтірілді. Nessus Vulnerability Scanner осалдықты анықтаудағы үздік сканер болып табылады. Басты артықшылығы – деректер базасындағы қауіпті моделдер негізінде желіні тез әрі сапалы тексереді.

Әдебиеттер

1. Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие // Ю. Н. Загинайлов. – М. Берлин: Директ-Медиа, 2015. – 253с.

2. Бова В.В. Концептуальная модель представления знаний при построении интеллектуальных информационных систем // Известия ЮФУ. Технические науки. – 2014. – № 7 (156). – С. 109–117.

3. Коломейцева А.Д., Загинайлов Ю.Н. Разработка концептуальной модели системы защиты государственной информационной системы // Анализ современных тенденций развития науки: сборник статей Международной научно - практической конференции, Волгоград, 5 июля 2017 г. – Уфа: АЭТЕРНА. В 2 частях. – Ч.1 – С. 41–44.

4. Симонова М.В., Атрощенко В.А. Особенности построения различных алгоритмов и функциональных моделей в системе мониторинга умного дома // VII международная научно-практическая конференция молодых ученых, посвященная 56-й годовщине полета Ю.А. Гагарина в космос: Сборник научных статей, Краснодар, 12-13 апреля 2017 г. - Краснодар: Общество с ограниченной ответственностью "Издательский Дом - Юг". – С. 420–424.

5. Shangytbayeva G. A., Karpinski M. P., Akhmetov B. S., Yerekesheva M. M. Zhekambayeva M. N. Mathematical Model of System of Protection of Computer Networks against Attacks DOS/DDOS [Электронный ресурс]. – Режим доступа: https://doi.org/10.5539/mas.v9n8p106, свободный (дата обращения: 31.08.2020 г.).

6. Новохрестов А.К. Модель угроз информационной безопасности программного обеспечения компьютерных сетей на основе атрибутивных метаграфов. Диссер.канд. техн. Наук. - Томск, 2018. – 114 с.

7. BugTraq.Ru: Модели механизмов реализации типовых угроз безопасности РВС [Электронный ресурс]. – Режим доступа: https://bugtraq.ru/library/books/attack/chapter03/02.html?k=9, свободный (дата обращения: 31.08.2020 г.).

8. Королёва О.Ю. Модель и метод оценки эффективности системы обеспечения информационной безопасности корпоративного хранилища данных кредитных организаций Российской Федерации // Автореф. дис. канд. техн. наук [Электронный ресурс]. – Режим доступа: http://aspirantura.ifmo.ru/file/other/ktyaZl1TkI.pdf, свободный (дата обращения: 31.08.2020 г.).

9. СТ РК ISO/IEC 27013-2017. Информационные технологии. Методы и средства обеспечения безопасности. Руководство по интегрированному внедрению ISO/IEC 27001 и ISO/IEC 20000-1. [Электронный ресурс]. – Режим доступа: https://online.zakon.kz/Document/?doc_id=37992086#pos=0;0, свободный (дата обращения: 01.09.2020 г.).

10. KZ-CERT. Компьютерлік инциденттерге әрекет ету қызметі. [Электронды ресурс]. – https://cert.gov.kz, (01.09.2020 г.).

11. THE NESSUS FAMILY. [Электронный ресурс]. – https://www.tenable.com/products/nessus, (07.09.2020 г.).

12. Безопасность. Локальная сеть. [Электронный ресурс]. – https://www.youtube.com/watch?v=oLyo1FFQjKs, (07.09.2020 г.).

МАТЕРИАЛЫ
V международной научно-практической конференции
"Информатика и прикладная математика",

29 сентября - 1 октября 2020, Алматы, Казахстан

Под редакцией М.Н. Калимолдаева

Компьютерная верстка
Шокишалов Ж.М.

Подписано в печать 25.09.2020 г. Формат А4
Печать цифровая. Бумага офсетная. Усл. печ. л. 70,8.
Тираж 300 экз. Заказ № 006686.
Отпечатано в ИИВТ МОН РК.
Алматы, ул. Пушкина, 125