ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2025»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2025»

PROCEEDINGS
of the XX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2025»

2025
Астана

УДК 001(06)
ББК 72я631
F96

«ǴYLYM JÁNE BILIM – 2025» студенттер мен жас ғалымдардың XX Халықаралық ғылыми конференциясы = XX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2025» = The XX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2025». – Астана: – 3813 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-08-5373-7

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.В сборник вошли доклады студентов, магистрантов, докторантов имолодыхученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001(06)
ББК 72я431
F96

ISBN 978-601-08-5373-7

Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 2025

СЕКЦИЯ 2

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ И КОММ УНИКАЦИОННЫЕ ТЕХНОЛОГИИ

Подсекция 2.2

Интеллектуальные информационные системы

255.	Сафонова Софья Александровна «Современные аспекты информационной безопасности в облачных вычислениях: модели, угрозы и методы защиты»	1034
256.	Смаилова Назгүл Батырбекқызы «Терең оқыту арқылы кітап ұсыныстарын әзірлеу: collaborative filtering, content-based және nlp әдістерінің комбинациясы»	1041
257.	Тажібай Аружан Айдосқызы, Кудубаева Сауле Альжановна «Көру қабілеті әлсіз адамдарға арналған аі дауыстық көмекші: нақты уақытта объектілерді анықтау және қашықтықты бағалау»	1046
258.	Тайжанов Азамат Жанкелдіұлы «Python тілінде фильмдердің интеллектуалды ұсыныс жүйесін әзірлеу»	1051
259.	Умирзахов Сундетали Кабылбекович «Сұраныстарды интеллектуалды талдау негізінде ұйымның сайты үшін чат-бот құру»	1055
260.	Шайхстан Марғұлан «IOT Сенсорлары негізінде ауа ластану деңгейін болжау»	1060

Подсекция 2.3

Современные тенденции в программной инженерии и управлении в условиях цифровой индустрии

261.	Bekenova A.B. «Development of a registration panel for users and doctors with integration into the database»	1077
262.	Bolat A.Zh. «Data analysis methods and decision making using big data and machine learning tools»	1081
263.	Алтайұлы А. «Visual studio интегралды ортасында «қойма қызметкерлеріне арналған» мәліметтер қорын жобалау»	1086
264.	Арап А.Қ. «Ақылды сурет салушы роботты әзірлеу»	1088
265.	Артыкбекқызы А. «Ақылды үйлердегі заттар интернеті(iot) мен робототехниканың өзара әрекеттесуі»	1091
266.	Ахметова А.Д. «Тоңазытқыштағы өнімдерді бақылауға және тағам әзірлеу ұсынысын беруге арналған программалық қосымша»	1096
267.	Дәрібай Д.Д. «Робототехниканы қолдану арқылы қойма логистикасындағы қолданыстағы басқару жүйелерін талдау»	1100
268.	Жамбулов С.Ж. «Білім алушыларды информатика және программалау олимпиадаларына дайындауда жасанды интеллекттің қолданысы»	1102
269.	Каиржан Р.С. «Development of system for recognition of emotional states of employees based on computer vision methods on Raspberry Pi»	1108
270.	Кайрекенова Н.Р. «Өнеркәсіптік роботты көру үшін машиналық оқытудың заманауи тәсілдері: әдістер, деректер жиынтығы және оптимизациялау»	1111

СЕКЦИЯ 3
ЕСТЕСТВЕННЫЕ НАУКИ

УДК 004

ҚАУІПСІЗДІК ИНЦИТЕНТТЕРІНЕ ҚАЛАЙ ЖАУАП БЕРУГЕ БОЛАДЫ?

Қажкен Елнұр Елібайұлы
elnrkazken@gmail.com
Темиржан Санжар Арманұлы
stoni7380@gmail.com

Теориялық математика институтының ғылыми қызметкері
және ғылыми есептеулер. Л. Н. Гумилева, Астана, Қазақстан
Ғылыми жетекшісі-Кавиева Н.М.

Қазіргі таңда ұйымдар өздерінің көптеген жұмыс процестерін технологияларға сеніп тапсырады. Алайда, бұл үрдіспен бірге ақпараттық қауіпсіздік (АҚ) инциденттерінің саны да артып келеді. Мұндай жағдайларға тек ірі корпорациялар ғана емес, шағын кәсіпорындар да тап болуда.

[1] Мақалада айтылғандай ақпараттық қауіпсіздік инциденті дегеніміз – бұл ұйымның ақпараттық жүйелерінің тұрақтылығына, құпиялылығына, тұтастығына және қолжетімділігіне қауіп төндіретін күтпеген немесе жағымсыз оқиға. Мысалы, қызметкердің компанияның қаржылық деректерін сыртқа жариялауы осындай инциденттердің бірі болып табылады.

Мұндай жағдайлар ұйымның IT-инфрақұрылымының қалыпты жұмысына кедергі келтіріп, елеулі тәуекелдерге әкеледі. Олардың ішінде операциялық бұзылулар, заңдық мәселелер, беделге нұқсан келтіру және қаржылық шығындар бар.

[1] Ақпараттық қауіпсіздікке қатысты қауіптер олардың түрлері мен маңыздылық деңгейіне қарай жіктеледі. Инциденттердің түрлері ISO/IEC 27035-1 халықаралық стандартына сәйкес бөлінеді. Бұл стандарт инциденттерді анықтау, талдау және оларға әрекет ету үшін жүйелі тәсілді қамтамасыз етеді.

ISO/IEC 27035-1 бойынша негізгі инцидент түрлері:

- Зиянды бағдарламалық қамтылыммен жұқтыру;
- Рұқсатсыз қол жеткізу;
- Ақпарат жинау әрекеттері;
- Ақпараттық қауіпсіздік саясатын бұзу;
- Жарамсыз мазмұндағы ақпаратты тарату.

Осылайша, ұйымдар үшін ақпараттық қауіпсіздік инциденттерін алдын алу және оларға тиімді әрекет ету маңызды міндет болып табылады.

Инциденттерді анықтау және жіктеу киберқауіпсіздікдің маңызды рөлі болып табылады. Тиімді қорғаныс үшін заманауи бақылау құралдарын қолдана отырып, оқиғаларды танып, жіктей білу қажет.

Ақпараттық қауіпсіздік оқиғаларының жіктелуі

Ақпараттық қауіпсіздік инциденттері мен жұмыс істеу кезінде олардың жіктелуі жақсы тәжірибе болып саналады. Инциденттер әдетте бөлінеді:

- түрлері бойынша,
- ұйымға сыни дәрежесі (немесе зиян келтіру дәрежесі) бойынша.

Түрлері бойынша жіктеу кезінде көбінесе нормативтік құжаттар мен стандарттарда сипатталған немесе ұйымдардың өздері анықтаған Санаттар қолданылады [2].

Бұл жұмыста біз негізгі 3 инцидентті қарастырамыз 1-кестеде көрсетілген.

1-кесте инциденттер түрлері.

Инциденттер түрлері	Сипаттамасы
Зиянды бағдарламалар	Компьютердің, желінің немесе пайдаланушының деректеріне зиян келтіру, оларды өзгерту, ұрлау немесе жүйенің қалыпты жұмысын бұзу мақсатында жасалған арнайы бағдарламалық қамтамасыз ету[6].
DDoS шабуылдар	Бұл-желіні, операциялық жүйені немесе қосымшаны олардың өңдей алатын мөлшерінен асып кететін трафик, қосылым немесе сұраулардың үлкен көлемімен толтыру әдісі[7].
Әлеуметтік инженерия	Адамдарды манипуляциялау әдісі, оның мақсаты – олардың құпия ақпаратын, ресурстарға қолжетімділігін немесе басқа да құнды объектілерді алу[8].

Бұл инциденттерді таңдаған себебіміз – олар кең таралған және қауіптілік деңгейі бойынша жоғары.

Бұл кезеңде инцидентті тану, анықтау және тіркеу жүзеге асырылады.

Кезекті мақалада оқығанымыздай ақпараттық қауіпсіздік инциденттерін бақылау — тіркеу және кейінгі талдау арқылы жүзеге асырылады. Мониторинг автоматтандырылған болуы мүмкін — мамандандырылған құралдарды (SIEM), қолмен немесе аралас, екі әдісті де қолдана отырып. SIEM туралы осы жұмыста жақсы жазылған[3].

Осы жұмыста біз мысал ретінде инцидентті тану, анықтау және тіркеу қалай жүзеге асырылатынын кесте-2 көрсетілген құралдарды қолданану арқылы көрсетеміз.

Кесте 2. Анықтау құралдары мен әдістері

Әдіс	Сипаттамасы
Желі мониторингі	Желідегі қалыптан тыс әрекеттерді анықтау үшін IDS/IPS жүйелерін (мысалы, Snort) пайдалану.
Журналдарды талдау	Windows Event Logs тексеру құрылғылардағы рұқсат етілмеген әрекеттерді анықтауға көмектеседі.
Файлдарды тексеру	VirusTotal[3] сияқты қызметтер күдікті файлдарда зиянды кодтың болуын анықтауға мүмкіндік береді.
Домендер мен IP мекенжайларын талдау	Whois, AbuseIPDB және VirusTotal шабуылдарда қолданылатын зиянды мекенжайларды анықтауға көмектеседі.

Ақпараттық қауіпсіздік инциденттеріне жауап беру жоспары.

Оқиғаларды тіркеу және құжаттау.

Жауап беру жоспары инциденттерді анықтап, оларға жауап беруді кім іске қосатынын көрсетуі керек. Инциденттердің маңыздылығы өңдеу жылдамдығы мен ресурстарды анықтайды. Құжаттарды жаңартып, кибершабуылдар мен хакерлік әдістерді зерттеу ұсынылады[4].

Әрбір негізгі топ мүшесінің рөлдері мен міндеттерін құжаттаңыз. Команданы оқытып, оның функцияларын сынақтан өткізіңіз.

Кәсіпорын инфрақұрылымын негізгі бағыттар бойынша талдау

Тәуекелдерді бағалау арқылы осал тұстарды анықтаңыз. Төмен және орташа тәуекелдер үшін жауап беру басымдылығын белгілеп, сипаттаңыз.

Инциденттерді жауап беру кезеңдері

Жоғары деңгейдегі жауап беру процесі мыналардан тұрады:

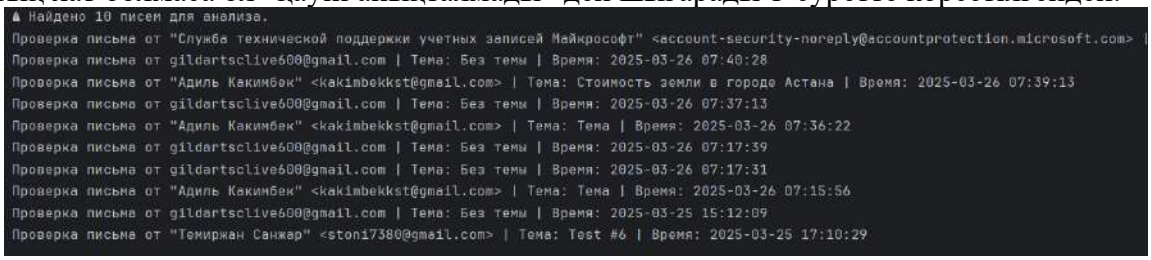
- Дайындық;

- Анықтау және талдау;
- Ұстау;
- Жою;
- Қалпына келтіру;
- Оқиғадан кейінгі қызмет.

Жауап беру процесітері туралы осы жұмыста [5] толығырақ жазылған.

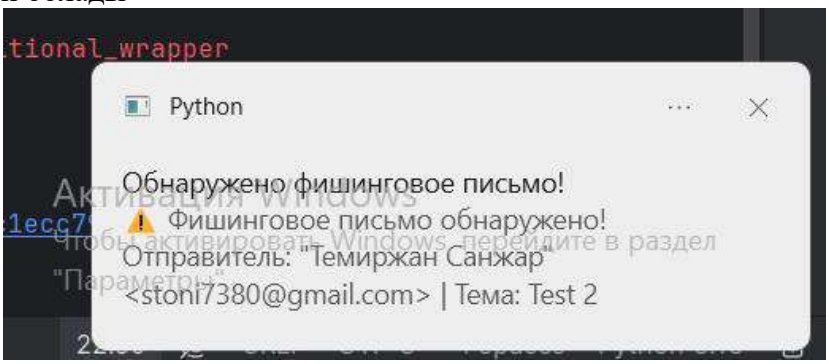
Ақпараттық қауіпсіздік инциденттерін өңдеу кезеңдері

Осы жұмыста біз тәжірибе ретінде қазіргі танда кенінен таралған фишингтық шабуылдарды анықтайтын бағдарлама жасадық. Онын негізгі міндеті электрондық почтаға gmail API арқылы қосылып почтаға келген хаттарды мазмұнын тексереді. Егерде почтада фишингтық хат болмаса ол “қауіп анықталмады” деп шығарады 1-суретте көрсетілгендей.



1-Сурет электронды почтаға келген хаттардың тізімі

Ал егерде анықталатын бола ол қауіп бар деп шығарады және оны қандай адрестен келгенін, қандай қауіп екенін көрсетеді және келген хатты жояды, хатты жіберген пайдаланушыны бұғаттайды. 2-суретте көрсетілгендей практикалық жұмыстың нәтижесінде хаттан зиянды бағдарлама анықталған жағдайда “Обнаружено фишинговое письмо!” деген хабарлама келетін болады



2-Сурет зиянды бағдарлама анықталған жағдай

Сосын зиянды бағдарламаларды жіберген пайдаланушылардың электрондық почталарын қай уақытта жібергенін json файл ретінде сақтайды және фишингтық сілтеме көрсетеді 3-суретте көрсетілген.

3-Сурет фишингтік хатты жіберуші туралы ақпараттар

Нәтижесінде бағдарлама фишингтік инцидентті сәтті анықтады және тиісті әрекеттерді орындады. Ең алдымен, жүйе келген хаттың мазмұнын мұқият талдап, ондағы күдікті элементтерді – фишингтік сілтемелерді, жалған жіберушіні және күмәнді тіркемелерді анықтады.Анықталған фишингтік хат жөнінде барлық қажетті ақпарат жүйеге тіркеліп, нәтижесінде. Жіберуші автоматты түрде бұғатталды, осылайша ол болашақта жаңа хабарламалар жібере алмайды.Зиянды хат пайдаланушының пошта жәшігінен толықтай жойылды, бұл оның кездейсоқ ашылу қаупін болдырмауға мүмкіндік берді. Фишингтік шабуыл туралы мәліметтер JSON файлына сақталды, онда хат жіберушінің электрондық пошта мекенжайы, хабарлама жіберілген уақыты, күмәнді сілтеме көрсетілген.

Қорытындылай келе қазіргі танда ұйымдар өздерінің тұрақты жұмысына, қаржылық тұрақтылығына және беделіне қауіп төндіретін ақпараттық қауіпсіздік оқиғаларына көп тап болады. Бұл жұмыста қауіп-қатерлерге жауап берудің негізгі аспектілері, соның ішінде оқиғалардың жіктелуі, оларды анықтау әдістері және салдарды жою стратегиясы қарастырылған.

Зерттеу ақпараттық қауіпсіздік оқиғалары әртүрлі сипатта болуы мүмкін екенін көрсетті – зиянды бағдарламалық жасақтама инфекциясы мен DDoS шабуылдарынан бастап ұйым қызметкерлерін манипуляциялауға бағытталған әлеуметтік инженерия әдістеріне дейін. Осы оқиғалардың әрқайсысы Siem жүйелері, оқиғалар журналын талдау және желілік трафикті бақылау сияқты кешенді шешімдерді қолданудың маңыздылығын растайтын жеке анықтау және жауап беру тәсілін қажет етеді.

Жұмыстың практикалық аспектілерінің бірі фишингтік шабуылдарды автоматты түрде анықтау әдістерін қарастыру болды. Кіріс хабарламаларды талдау және ықтимал қауіптерді анықтау үшін Gmail API қолданатын бағдарлама жасалды. Бұл құрал фишингтік хаттарды анықтап қана қоймай, күдікті хабарламаларды жою және олардың жіберушілерін бұғаттау сияқты жедел шаралар қабылдауға мүмкіндік береді.

Бұл зерттеудің нәтижелері киберқауіпсіздікке кешенді көзқарастың қажеттілігін көрсетеді. Технологиялық шешімдердің, тәуекелдерді сауатты басқарудың және қорғаныс процестерін үнемі жетілдірудің арқасында ғана ұйымдарға киберқауіптерге тиімді қарсы тұруға және олардың жағымсыз салдарын азайтуға мүмкіндік береді.

Пайдаланылған әдебиеттердің тізімі

1. Инциденты информационной безопасности: что это, расследование и порядок реагирования // https://www.klerk.ru/blogs/laboratoria_kasperskogo/630561/#chapter-chto-takoe-incident-i-sobytie-informacionnoy-bezopasnosti (дата обращения: 23.03.2025)

2. Инциденты информационной безопасности: выявление, расследование и реагирование // https://selectel.ru/blog/security-incidents/ (дата обращения: 23.03.2025)
3. Что такое SIEM ? // https://www.microsoft.com/ru-ru/security/business/security-101/what-is-siem (дата обращения: 25.03.2025)
4. План реагирования на инциденты кибербезопасности: что это и почему он нужен каждой организации // https://ddos-guard.ru/blog/plan-reagirovaniya-na-incidenty-kiberbezopasnosti (дата обращения: 25.03.2025)
5. Отакулов Артур Собирович Способы реагирования на инциденты информационной безопасности // E-Scio. 2020. №1 (40). URL: https://cyberleninka.ru/article/n/sposoby-reagirovaniya-na-intsidenty-informatsionnoy-bezopasnosti (дата обращения: 31.03.2025).
6. Русскевич Евгений Александрович Понятие вредоносной компьютерной программы // Актуальные проблемы российского права. 2018. №11 (96). URL: https://cyberleninka.ru/article/n/ponyatie-vredonosnoy-kompyuternoy-programmy (дата обращения: 31.03.2025).
7. Голубятников Артем Олегович DDOS-АТАКИ И МЕТОДЫ БОРЬБЫ С НИМИ // E-Scio. 2022. №10 (73). URL: https://cyberleninka.ru/article/n/ddos-ataki-i-metody-borby-s-nimi (дата обращения: 31.03.2025).
8. Что такое социальная инженерия ? // https://www.kaspersky.ru/resource-center/definitions/what-is-social-engineering (дата обращения: 31.03.2025)

УДК 004.056

MITM ШАБУЫЛЫ (АДАМНЫҢ ОРТАДАҒЫ ШАБУЫЛЫ)

Қартбай Елнұр Ғалымжанұлы
Тынарбай Назым Исламбекқызы
shattik59@gmail.com,tynarbayn@gmail.com
Л.Н.Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультеті
Ақпараттық қауіпсіздік жүйелері кафедрасының студенттері, Астана, Қазақстан
Ғылыми жетекші: Казиева Назым Магидулловна

Аңдатпа

Бұл мақалада Man-in-the-Middle (MITM) шабуылының негізгі түрлері, орындалу механизмдері және олардың қауіпсіздікке тигізетін ықпалы қарастырылған. MITM шабуылы желідегі деректер алмасуға араласу арқылы ақпаратты ұрлау немесе өзгертуге мүмкіндік береді. MITM шабуылын жүзеге асыру үшін ARP-spoofing, DNS-spoofing, SSL-stripping сияқты әдістер кеңінен қолданылады. Бұл зерттеу аясында Kali Linux жүйесінде Bettercap құралы арқылы ARP-spoofing шабуылының орындалу тәсілдері зерттеліп, трафикті ұстап алу және өзгерту процестері көрсетілген. Сонымен қатар, MITM шабуылынан қорғану жолдары, HTTPS, VPN, ARP-қорғаныс механизмдері және жүйелік қауіпсіздік шаралары талданды. Бұл зерттеу MITM шабуылдарының механизмдерін тереңірек зерттеу негінде желілік қауіпсіздікті күшейту бағыттары анықталған.

Кілт сөздер: MITM шабуылы, ARP-spoofing, Kali Linux жүйе, Better Cap құралы, желілік қауіпсіздік.

Кіріспе. Қазіргі таңда ақпараттық қауіпсіздік кибершабуылдардың қарқынды дамуына байланысты маңызды мәселелер туындалуда. Ақпараттық технологиялардың дамуы "Man-in-the-Middle" (MITM) шабуылының жиі орын алуына ықпал етеді. Бұл шабуыл кезінде қаскүнем