

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

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

**Студенттер мен жас ғалымдардың
«ҒҮЛЫМ ЖАҢЕ БІЛІМ - 2025»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ**

**СБОРНИК МАТЕРИАЛОВ
XX Международной научной конференции
студентов и молодых ученых
«ҒҮЛЫМ ЖАҢЕ БІЛІМ - 2025»**

**PROCEEDINGS
of the XX International Scientific Conference
for students and young scholars
«ҒҮЛЫМ ЖАҢЕ БІЛІМ - 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, докторанттардың 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 и молодых ученых 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

		сауаттылығын арттыру	
203.	Эрболат А.	Орта мектепте нанотехнология ұғымын оқытудың тиімді әдістері	808

СЕКЦИЯ 2

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ И КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

Подсекция 2.1			
Цифровая трансформация образования			
204.	Адалбек Н.	«Традиционные и интеллектуальные подходы в обучении»	812
205.	Бакенова А.А.	«Цифровизация тестирования: разработка нейросетевого приложения для формирования заданий по английской грамматике»	816
206.	Бекмурат А.Е.	«Инновационные методы обучения информатике в школе на основе искусственного интеллекта»	821
207.	Назарова А.Т.	«Развитие цифровых компетенций учителей в условиях персонализированного обучения»	826
208.	Нуриева Д.Р.	«Цифровая трансформация педагогики: роль информационных технологий в повышении квалификации преподавателей»	830
209.	Абдуашимова П.М.	«Білім беру процесінде жасанды интеллект технологияларын қолданудың тиімділігі»	833
210.	Ажибаева А.Д.	«Мектеп информатикасын оқытудағы кемшіліктерді жою жолдары»	837
211.	Асылбек М.А.	«Орта мектепте білім беру үдерісінде үлкен деректерді қолдану әдістемесі»	842
212.	Аталова А.Е.	«Әлеуметтік желілерді информатика пәні бойынша оқыту құралы ретінде пайдалану»	845
213.	Балтабаев Н.П.	«Мектептерде сабақ кестесін автоматтандыруға арналған интеллектуалды жүйе құру»	851
214.	Балтабаев Н.П., Дәрменов Ә.М., Мұратова М.М.	«Жасанды интеллект негізінде жаратылыстану пәндерін оқытуды жетілдіру: BilimALL AI платформасының мүмкіндіктері»	854
215.	Баумуратова Х.Б.	«АКТ оқыту барысында бастауыш сынып оқушыларының цифрлық сауаттылықтарын қалыптастырудың әдістемесі»	856
216.	Баумуратова Ш.Б.	«Жасанды интеллект негізінде инклюзивті білім беруді жетілдіру»	859
217.	Ғазиз Ж.Е.	«Бастауыш мектепте ақпараттық-коммуникациялық технологияларды оқыту әдістемесі»	863
218.	Дәрменов Ә.М.	«Информатиканы қолжетімді ететін мобильді "BilimAll" қосымшасы»	866
219.	Дүйсегалиева Н.А.	«HIGH-TOUCH HIGH-TECH моделі арқылы болашақ информатика мұғалімдерін машиналық оқыту негізінде даярлаудың	870

	инновациялық тәсілдері туралы»	
220.	Еликбай А.Ж. «Ақпараттық дәуірде білім берудің жаңа кезеңі – Инфографика»	874
221.	Жаңабекқызы А. «EDCAFE AI көмегімен сабақты жоспарлау»	879
222.	Жумабекова У.Б., Сабырова М.Е., Сабыров Т.С. «Информатика пәнін жобалап оқыту технологиясы»	883
223.	Кендебай Н.А. «EDUVISION білім беру процесін қадағалайтын қосымша»	888
224.	Көшенова А. «Цифрлық сауаттылықтың мектеп курсы бойынша интеллектуалдық оқу басылымдарына арналған дидактикалық материалдар»	891
225.	Куанышева Д.Ж. «Инклюзивті білім беруде педагогтың ақпараттық-коммуникациялық технологияларды (АКТ) қолдану даярлығын жетілдіру»	893
226.	Мауленова М.А. «Үлкен деректерді өңдеуде машиналық оқытудың әдістері мен құралдары»	897
227.	Мылтыкбаева Ж.Т. «Жаратылыстану пәндерін STEM білім беру мен ROS операциялық жүйесі негізінде кешенді оқыту»	901
228.	Надирхан Г.Е. «Ауыл мектептерінде цифрлық оқытуды дамыту мүмкіндіктері»	903
229.	Орынбаев М.Ж. «Компьютерлік көру алгоритмдерін машиналық оқыту негіздері бойынша қолданудың оқу-әдістемелік негіздері»	907
230.	Сабитова А.Б., Ражапова А.Н. «Жасанды интеллект және білім: болашақ мұғалімдерге арналған жаңа мүмкіндіктер»	910
231.	Сағындықова А.С. «Болашақ информатика мұғалімдерін магистратураға даярлаудағы онлайн-курстардың рөлі»	915
232.	Сайлау Ж.Б. «Халықаралық зерттеуге оқушыларды АКТ арқылы дайындаудағы педагогтердің құзыреттілігін арттыру жолдары»	918
233.	Төрәлі Қ.Н. «Бастауыш сынып оқушыларының цифрлық сауаттылығын дамытудың ерекшеліктері»	923
234.	Турмаганбетова З.П., Алтыбаева А.Н. «Ерекше білімді қажет ететін оқушыларға мектеп информатика курсы оқытуды ұйымдастыру»	927
235.	Халхабай А. ««Алгоритмдеу және бағдарламалау» курсы бойынша мобильді қосымшаны оқу үдерісінде қолдану»	931
236.	Ысмайыл Н. «Мектеп информатика курсына жобалық оқыту әдісін енгізу»	936
237.	Избасарова М.Р. «Білім берудегі тестілеу жүйелері»	938

Подсекция 2.2

Интеллектуальные информационные системы

238.	Amantayeva Gulden Turarkyzy «Comparative analysis of models and methods in heart disease prediction problems»	944
------	---	-----

239.	Tanirbergenov Meirbek Sagyndykovich «Facial Recognition-Based Attendance Management»	947
240.	Toleubay Daniyar Manatuly «Cardiac disease prediction using machine learning algoritms»	952
241.	Yerezhepov Rakhat Aibulatovich «Detecting logical fallacies in web content with nlp-powered crawling»	957
242.	Ажикенов Арман Русланович, Абашев Арслан Азатабекович «Оптимизация дорожного трафика в Астане через симуляцию транспортных потоков»	962
243.	Аманжол Альфараби Маликович, Сабит Мадияр, Кушербаев Бекзат Алибекулы «Система визуализации и анализа данных о передвижении нефти на основе интерактивной карты»	968
244.	Аскапова Мадина Куанышбековна «Параллельді қазақ-түрік сөйлеу корпусы қалыптастырудың әдісі мен моделін құру»	972
245.	Бекқожин Дастан Ақанұлы «Терең оқыту негізінде қолжазба таңбаларын тану программалық құралын әзірлеу»	975
246.	Дакенов Алишер Мырзахметұлы «Анализ сигналов ЭЭГ нейросетевыми методами для ранней диагностики нейродегенеративных заболеваний»	978
247.	Доспол Нәзгүл Нурланқызы, Жеткенбай Лена «Балабақшадағы балалардың эмоциялық жағдайын бақылауға арналған эмоцияларды тану жүйесін әзірлеу»	987
248.	Ермекбай Айболат, Молдабек Елжан «Жасанды интеллект негізінде веб-қосымша әзірлеу»	992
249.	Жұмал Жания Ержанқызы, Абдурахман Жансая Берікжанқызы «Применение голосового ИИ-помощника в геймифицированной образовательной среде»	1001
250.	Каримов Руслан Жасинович «Эффективность существующих ИИ-решений в основных направлениях транспортной логистики»	1007
251.	Кубиева Сабина Талгатовна, Утепбергенова Зарина Арманкызы «Разработка iot системы по уходу за растениями на базе искусственного интеллекта»	1012
252.	Кудобаев Даниал Дулатович «Разработка информационной системы для автоматизации стоматологических услуг»	1017
253.	Мусина Данель Тлеухановна «Интеллектуальные инструменты автоматизированной диагностики надежности информационных систем»	1024
254.	Рогова Ксения Александровна, Қабдыбек Ризат Досмжанұлы, Джумадиева Тогжан Бекежановна «Мониторинг инженерных конструкций на основе искусственного интеллекта»	1030

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 ai 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

271.	Калижан А.К. «Разработка системы биометрической аутентификации с предотвращением deepfake атак»	1113
272.	Касылкасова К.Н. «Программное обеспечение smartmed для обработки медицинских данных и диагностики»	1118
273.	Қабдешев Ә.Е. «Жөтелді талдау негізінде денсаулықты диагностикалаудың интеллектуалды программасын әзірлеу»	1120
274.	Махаев Е.Е. «Разработка облачного приложения для автоматизации деятельности сети аптек»	1123
275.	Муратов М.М. «Эффективность единой информационной системы агропромышленного комплекса»	1126
276.	Нуржанова А.Б. «Современные методы классификации эмоций: анализ подходов и перспективы развития»	1130
277.	Нурпеисова З.Р. «Обзор и исследование методов искусственного интеллекта для анализа рынка недвижимости»	1134
278.	Рақымбек А.С. «Кітапқұмарларға арналған платформа: кітаптарды оқу және бөлісу үшін әлеуметтік желіні жобалау және іске асыру»	1138
279.	Сагидуллина Д.С. «Visual studio интегралды ортасында «қаржылық транзакцияларды қадағалау және талдауға арналған» мәліметтер қорын жобалау»	1144
280.	Төлеубай Д.М. «Yolov10 қолдану арқылы рентген суреттерінде сүйек сынуын анықтауды кешенді зерттеу»	1147
281.	Утегенова Д.Б. «Visual studio интегралды ортасында «фитнес орталық қызметкері үшін» мәліметтер қорын жобалау»	1152
282.	Шаймуратов А.Ж. «Проектирование аппаратно-программного комплекса для автоматизированного учета железнодорожного подвижного состава»	1154
Подсекция 2.4		
Информационная безопасность		
283.	Akniyet N. «Smart home automation and security system using arduino uno r4 and esp32 microcontrollers with telegram integration»	1158
284.	Askhatov A. «Analysis of social engineering methods and development of a defense strategy for corporate structures»	1165
285.	Bekturganov A.B. «Development of an early detection model for ddos attacks based on network traffic analysis»	1170
286.	Gabdullin A. «Analysis of modern wireless network security protocols and prospects for their development»	1174

287.	Garifullin A. «Modern information security management systems: construction and implementation in the digital era»	1179
288.	Igumenshev D.V. «Methods of embedding malicious code into pdf files»	1182
289.	Issabay T.B. «Utilizing sandboxes for cybersecurity training: a hands-on approach»	1187
290.	Kalybayev S. «Overview of modern authentication methods in telecommunication systems: from passwords to biometrics»	1191
291.	Kerim A. «Owasp top 10 and alternative methods of its compilation»	1194
292.	Yergazin A. «Analysis of a protection of hybrid intrusion detection and prevention system (idps) for low-latency 5g networks with adaptive learning using edge computing»	1199
293.	Yerzhanova Y.Y. «Key attacks in web forensics: xss, sql injection and rce»	1204
294.	Zhakay A. «Fundamentals of modern cryptography: from encryption to digital signatures»	1209
295.	Айдарова А.А. «Visualvm көмегімен cast-128 және kuznyechik блоктық шифрларының кілт генерациясын салыстыру және стандарттарға шолу»	1214
296.	Акимбекова Д.М., Каиржанова Д.Ж. «Жергілікті желінің қауіпсіздігін қамтамасыз ететін негізгі параметрлер»	1220
297.	Аскарлов А.Д. «Разработка и исследование эффективности метода и инструмента для выявления фейковых новостей в социальных сетях»	1224
298.	Ауесхан Н. «Аномалияларды анықтау әдістерін талдау»	1229
299.	Ерболатов А. «Анализ вредоносных программ с помощью ии и криптографическая защита»	1332
300.	Ерболатова А.Ж. «Neuvecton және kubernetes: контейнерлік ортадағы қауіпсіздікті қамтамасыз ету тәсілдері»	1336
301.	Жанатаев М.К. «Стеганография на основе lsb: реализация сокрытия данных в медиафайлах»	1338
302.	Жарасхан Н.Ж., Қайупов Е.К. «Crystals-kyber алгоритмін ресурсы шектеулі құрылғыларға оңтайландыру»	1343
303.	Жолдасбаев М.Ә. «Заманауи операциялық жүйелердегі жады дампы кескінін алу құралдарын талдау және салыстыру»	1348
304.	Жолмұратұлы Б., Маратов Ә.Б., Ховдабай Н.А. «Екі факторлы	1353

	аутентификацияның қауіпсіздігі және оның қолданылуы»	
305.	Кадринов Д.М. «Автоматизация внедрения альтернативной soag платформы на основе средств со свободной лицензией»	1357
306.	Казбаганбетова М.А. «Wireshark бағдарламасын пайдаланып желілік трафикті талдау және ақпараттық қауіпсіздікті қамтамасыз ету»	1361
307.	Кәкімбек Ә.Қ., Серікбай А.Е., Наурызбаев Д.Е. «MITM шабуылы туралы»	1366
308.	Кеттеш Б.Н. «ELF талдауындағы capstone: сызықтық және рекурсивті дизассемблерлеу»	1370
309.	Көшкінбаева Ф.Қ. «Linux қорғаудың заманауи әдістеріне талдау.openvas және nmap көмегімен осалдықтарды анықтау»	1374
310.	Қадыр Н.Е. «Заманауи фишинг түрлері мен олардың ұйымдық ақпараттық жүйелерге ықпалы»	1379
311.	Қажкен Е.Е., Темиржан С.А. «Қауіпсіздік инциденттеріне қалай жауап беруге болады?»	1384
312.	Қартбай Е.Ғ., Тынарбай Н.И. «MITM шабуылы (адамның ортадағы шабуылы)»	1388
313.	Маратов Б.Ж. «Әлеуметтік инженерия қауіпсіздікке қатер ретінде: қызметкерлерді қорғау және оқыту әдістері»	1393
314.	Мағзумов А.М. «Websocket протоколындағы осалдықтарды талдау»	1397
315.	Майданов А.С. «Автоматизация процесса анализа оперативной памяти с использованием python»	1401
316.	Мақсат Ә., Нурсейтов С. «Блокчейн қажеттілік пе, әлде сән бе?»	1406
317.	Қ. Мырзағалиұлы. «Инциденттерді анықтауда желілік логтарды талдаудың маңызды рөлдері»	1409
318.	Нурбатуров С.К. «Интеграция honeypot в ит-инфраструктуру компании»	1412
319.	Нуриева Д.Р., Исайнова А.Н. «Анализ рисками безопасности данных в медицинских учреждениях»	1415
320.	Нұрлан А.Т. «Кескіндердегі статистикалық стегоанализ әдістері»	1420
321.	Оралбеков Е.А. «Ddos-шабуылдардың жаңа буыны»	1424

322.	Рамазанова Ж, Нұрлан А, Жайсанбаева А. «Бұлтты технологияларды пайдалану кезіндегі тәуекелдер мен қауіпсіздік шараларын зерттеу»	1430
323.	Сахатбекқызы Т., Бахтиярқызы Т.А. «IoT құрылғыларының желідегі қауіпсіздігін қалай қамтамасыз етуге болады: стратегиялар және packet tracer көмегімен модельдеу»	1434
324.	Серғазы М. «Повышение производительности разработчиков с помощью интегрированных искусственных интеллектов и соображения кибербезопасности»	1440
325.	Султанов А.М. «Стеганография в кибербезопасности казахстана»	1443
326.	Танатаров Е., Іргебай С., Султанов А. «WI-FI желісінде шақырылмаған қонақтарды автоматты түрде анықтау жүйесі»	1447
327.	Таубай М.Е. Рамагуллаев Ә.А. «Фишинг: желідегі beef әдісі арқылы алдау және одан сақтану»	1452

СЕКЦИЯ 3 ЕСТЕСТВЕННЫЕ НАУКИ

		ПОДСЕКЦИЯ 3.1 АКТУАЛЬНЫЕ ПРОБЛЕМЫ СОВРЕМЕННОЙ БИОЛОГИИ	
328.	Акимкара А.Б.	Гербарийдің ботаникалық зерттеулерде қолданылуы және гербарий қорындағы кеппе шөптің қалыптасу ерекшеліктері	1457
329.	Ақылбек А.	Астана қаласындағы ботаникалық бағының ландшафттағы <i>geranium sanguineum</i> биологиялық ерекшеліктеріне сипаттама беру	1459
330.	Әділхан Ж.	Мобильді байланыс пен қолданбалардың адамның мінез-құлқына әсерін анықтау	1463
331.	Базарбаева Қ.	Жасөспірімдерде девиантты мінез-құлықтың даму қаупі	1467
332.	Байдосова А.Б.	Методика использования игровых технологий на уроках биологии	1471
333.	Байдосова А.Б.	Актуальные проблемы современной биологии с использованием игровых технологий в образовании	1474
334.	Ғазизова Ә.	Сәулеленген егеуқұйрықтардың бүйректеріндегі морфофункционалдық өзгерістерді салыстырмалы бағалау	1477
335.	Еркін З.Б.	Биология сабақтарында оқушылардың сыни ойлау қабілетін жетілдіруде блум таксономиясын пайдалану	1482
336.	Жанабергенова	Кенеттен жүрек өлімі: генетикалық аспектілері	1486

ҚАУІПСІЗДІК ИНЦИДЕНТТЕРІНЕ 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 киберқауіпсіздіктің 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. Ициденттер 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:

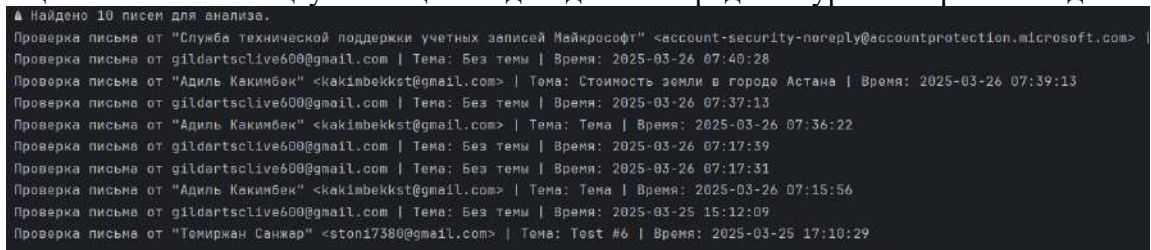
- Дайындық;

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

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

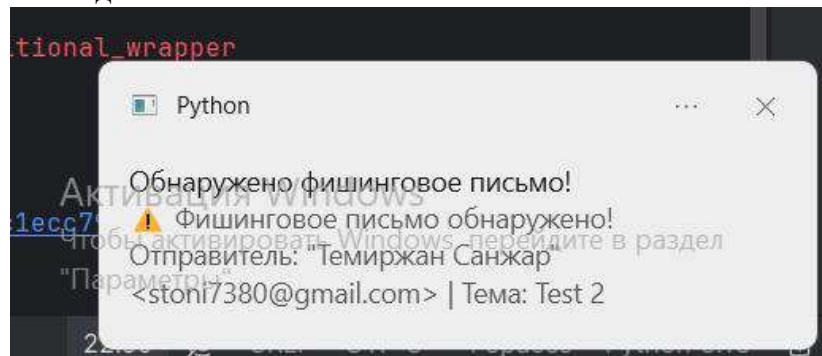
Ақпараттық қауіпсіздік инциденттерін өңдеу кезеңдері

Осы жұмыста біз тәжірибе ретінде қазіргі таңда кенінен таралған фишингтық шабуылдарды анықтайтын бағдарлама жасадық. Оның 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 адресстен 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.

```
1 [
2   {
3     "sender": "\"Темиржан Санжар\" <stoni7380@gmail.com>",
4     "subject": "Test 2",
5     "date": "2025-03-31 11:14:18",
6     "phishing_links": [
7       "https://maoffinle.wixsite.com/maioffilse"
8     ]
9   }
10 ]
```

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 таңда 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-cto-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 Собинович 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 процесі көрсетілген. Сонымен қатар, MITM шабуылынан қорғану жолдары, HTTPS, VPN, ARP-қорғаныс механизмдері және жүйелік қауіпсіздік шаралары талданды. Бұл зерттеу MITM шабуылдарының механизмдерін тереңірек зерттеу негізінде 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