

№	«6B06306 – Ақпараттық қауіпсіздік жүйелері» білім беру бағдарламасы Дипломдық жұмыстарының тақырыптары		
	Қазақ тілінде	Орыс тілінде	Ағылшын тілінде
1.	Сымсыз желілердің қауіпсіздігін қамтамасыз ету әдістері	Методы обеспечения безопасности в беспроводных сетях	Methods of ensuring the security of wireless networks
2.	SQLmap арқылы ақпарат алу үшін SQL инъекциясын зерттеу	Исследование SQL-инъекции для извлечения информации посредством SQLmap	SQL Injection research for information extraction via SQLmap
3.	Golang программалау тілінде әлеуметтік желілердегі ақпаратты қорғау әдістері	Методы защиты информации в социальных сетях на языке программирования Golang	Methods for protecting information in social networks in the Golang programming language
4.	Әр түрлі жағдайдағы Windows операциялық жүйелерінің толық қауіпсіздігі	Полная безопасность операционных систем Windows в различных ситуациях	Complete security of Windows operating systems in various situations
5.	Веб-қосымшалардағы қауіпсіздікке қатер төндіретін спам және жарнамалық ақпаратты блоктауға арналған клиенттік программаны әзірлеу	Разработка клиентской программы для блокировки спам и рекламной информации, представляющей угрозу безопасности в веб-приложениях	Development of a client program for blocking spam and advertising information that poses a security threat in web applications
6.	Лог файлдарының көмегімен web-жүйелерді қорғау	Защита web-систем с помощью лог-файлов	Protection of web systems by using log files
7.	Веб-қосымшаларға шабуыл жасауға арналған құралдарды талдау.	Анализ инструментов предназначенных для атаки веб-приложений.	Analysis of tools designed to attack web applications

8.	Ақпараттық қауіпсіздік инциденттерін анықтау үшін Wireshark арқылы желілік трафикті талдау	Анализ сетевого трафика посредством Wireshark для определения инцидентов информационной безопасности	Analysis of network traffic through Wireshark to identify information security incidents
9.	Киберқауіпсіздікте стеганографияны қолдану	Применение стеганографии в кибербезопасности	Application of steganography in cybersecurity
10.	OSI моделінің желілік және транспорттық деңгейлерінде маршрутизаторлар мен брандмауэрлердің қауіпсіздігін қамтамасыз ету	Обеспечение безопасности маршрутизаторов и брандмауэров на сетевом и транспортном уровнях модели OSI	Ensuring the security of routers and firewalls at the network and transport levels of the OSI model
11.	WEB-беттерді сайттаралық скриптингтен қорғау	Защита WEB-страниц от межсайтового скриптинга	Protecting WEB-pages from cross-site scripting
12.	Ақпараттық технологиялар саласындағы компаниялар үшін ақпараттық қауіпсіздікті қамтамасыз ету әдістерін зерттеу	Исследования методов обеспечения информационной безопасности для компаний в сфере информационных технологий	Research of information security methods for companies in the field of information technology
13.	Кәсіпорында IT инфрақұрылымын дамыту бойынша корпоративтік стандартты әзірлеу	Разработка корпоративного стандарта по развитию IT инфраструктуры на предприятии	Development of a corporate standard for the development of IT infrastructure at the enterprise
14.	Нейро-бұлдыр желілерді қолдана отырып, ақпараттық қауіпсіздік жүйелеріне арналған құралдарды зерттеу	Исследование инструментария для систем информационной безопасности с использованием нейро-нечётких сетей	Research of tools for information security systems using neuro-fuzzy networks
15.	"Цесна-Астық" Концерні кәсіпорнын қорғаудың программалық жүйесін әзірлеу	Разработка программной системы защиты на предприятии Концерн «Цесна-Астык»	Development of a software protection system at the Concern "Tsesna-Astyk"
16.	Клиент желісінің топологиясындағы осалдықты зерттеу	Исследование уязвимости в топологии сети клиента	Vulnerability investigation in the client's network topology

17.	Facebook мысалында желілік байланыс жағдайында жеке тұлғаның ақпараттық қауіпсіздігі	Информационная безопасность личности в условиях сетевой коммуникации на примере Facebook	Information security of the individual in the conditions of network communication on the example of Facebook
18.	Мобильді пайдаланушылардың VPN сеанстарының ағып кетуінен қорғау құралдарын зерттеу және әзірлеу	Исследование и разработка средств защиты от утечек сеансов VPN мобильных пользователей	Research and development of means of protection against leakage of VPN sessions of mobile users
19.	Kali Linux операциялық жүйесінің құралдары арқылы енгізе тестілеу жүргізу	Проведение тестирования на проникновение посредством инструментов операционной системы Kali Linux	Penetration testing using Kali Linux operating system tools
20.	Nikto website vulnerabilities scanner көмегімен осалдықтарды зерттеу	Исследование уязвимостей с помощью Nikto website vulnerability scanner	Vulnerabilities investigating with Nikto website vulnerability scanner
21.	Автоматтандырылған кәсіпорын жүйесінде ақпаратты фишингтен қорғау әдістерін зерттеу және әзірлеу	Исследование и разработка методики защиты информации от целевого фишинга в автоматизированной системе предприятия	Research and development of methods for protecting information from spear phishing in an automated enterprise system
22.	Кәсіпорындағы ақпараттық жүйелердің ақпараттық қауіпсіздігінің аудит әдістемесі	Методика аудита информационной безопасности информационных систем на предприятии	Methodology of information security audit of information systems at the enterprise
23.	PostgreSQL жүйесінде деректерді қорғау әдістері мен құралдары	Методы и средства обеспечения безопасности данных в PostgreSQL	PostgreSQL data security methods and tools
24.	Зиянды программалық қамтаманы жедел жад ішінде анықтау	Обнаружение вредоносного программного обеспечения в оперативной памяти	Detection of malicious software inside RAM
25.	Security information and event management жүйесін қолдана отырып, ақпараттық қауіпсіздікті қамтамасыз ету әдістерін әзірлеу	Разработка методов обеспечения информационной безопасности с использованием системы Security information and event management	Development of methods for ensuring information security using the Security information and event management system

26.	Қауіпсіздік жүйесін әзірлеу кезінде биометриялық деректерді пайдалану	Использование биометрических данных при разработке системы безопасности	Use of biometric data in the development of a security system
27.	Vpn технологиясын қолдана отырып кәсіпорынның корпоративтік желісінің қауіпсіздігін қамтамасыз ету	Обеспечение безопасности корпоративной сети предприятия с применением технологии VPN	Ensuring the security of the corporate network of the enterprise using VPN technology
28.	Корпоративтік желілерде ddos-шабуылдардан ақпаратты қорғау құралдарын әзірлеу	Разработка средств защиты информации в корпоративных сетях от ddos-атак	Development of means of protecting information in corporate networks from ddos attacks
29.	Kali Linux құралдарының көмегімен Windows 10 ОЖ-нің осалдығын талдау және енуін тестілеу	Анализ уязвимостей и тестирование на проникновение ОС Windows 10 с помощью инструментов Kali Linux	Windows 10 Vulnerability Analysis and Penetration Testing with Kali Linux Tools
30.	Желі қауіпсіздігі мақсатында сымсыз желілерде ойын теориясын пайдалану	Использование теории игр в беспроводных сетях в целях сетевой безопасности	Using Game Theory in Wireless Networks for Network Security
31.	Интернет дүкеннің қауіпсіздік жүйесін әзірлеу	Разработка системы безопасности интернет магазина	Development of online store security systems
32.	Веб-қосымшаларда сеанс құруды зерттеу	Исследование создания сессии в веб приложениях	Explore on session creation in web applications
33.	Ақпараттық қауіпсіздік мәселелерін шешудің параллельді алгоритмдерін құру	Разработка параллельных алгоритмов для решения задач защиты информации	Development of parallel algorithms for solving information protection tasks
34.	Ақпараттық-коммуникациялық инфрақұрылымға шабуыл түрлерін талдау	Анализ видов атак на информационно-коммуникационную инфраструктуру	Analysis of types of attacks on information and communication infrastructure
35.	Жұмыс станцияларын кешенді қорғау	Комплексная защита рабочих станций	Comprehensive protection of workstations

36.	BGP-Hijack негізіндегі фишингтік шабуылдарды анықтау әдістерін талдау	Анализ методов выявления фишинговых атак на базе BGP-Hijack	Analysis of methods for detecting phishing attacks based on BGP-Hijack
37.	Dll SideLoading осалдығын пайдалану арқылы жүйеге енгізілген зиянды программаларды іздеуді автоматтандыру	Автоматизация поиска вредоносных закрепленных в системе с помощью эксплуатации уязвимости Dll SideLoading.	Automatization of the search for malware embedded in the system by exploiting the Dll SideLoading vulnerability.
38.	«Introduction to Cybersecurity» курсының әзірлеуі	Разработка курса «Introduction to Cybersecurity»	Develop the course «Introduction to Cybersecurity»
39.	Программалық қамтаманы әзірлеу кезінде ақпараттық қауіпсіздікті қамтамасыз ету (DevSecOps)	Обеспечение информационной безопасности при разработке ПО (DevSecOps)	Ensuring information security in software development (DevSecOps)
40.	Веб қосымшалардың аутентификациясындағы осалдықтар мен әлсіздіктер	Уязвимости и недостатки аутентификации веб приложений	Vulnerabilities and weaknesses in web application authentication
41.	Биометриялық аутентификацияны пайдалана отырып, «Bloom» ЖШС Интернет-дүкенінің қорғалған қосымшасын әзірлеу	Разработка защищенного приложения интернет-магазина ТОО «Bloom» с использованием биометрической аутентификации	Development of a secure application for the «Bloom» LLP online store using biometric authentication
42.	КиберСтраж” кешенінің көмегімен ақпараттық қауіпсіздік мониторингі	Мониторинг информационной безопасности с помощью комплекса “КиберСтраж”	Information security monitoring using the CyberGuard complex
43.	Ұйымдағы ақпараттық қауіпсіздік инциденттерін басқару	Управление инцидентами информационной безопасности в организации	Management of information security incidents in the organization
44.	HTTP серверін DDoS шабуылдарынан қорғау құралын жасау	Разработка средства защиты HTTP сервера от DDoS-атак	Development of means of protecting an HTTP server from DDoS attacks

45.	DDoS шабуылдарының әсерінен АҚЖ-не төнетін қауіпті анықтау және жою әдісін жасау	Разработка способа выявления и устранения угроз к СИБ при действии DDoS -атак	Development of a method for identifying and eliminating threats to the ISS during DDoS attacks
46.	Деректер базасына төнетін қауіптер түрлері және олардан қорғану әдістерін талдау	Типы угроз для базы данных и анализ методов защиты от них	Types of threats to the database and analysis of methods of protection against them
47.	Медициналық мекеменің ақпараттық жүйесінің қауіпсіздік саясатын құру	Построение политики безопасности информационной системы медицинского учреждения	Building a security policy of the information system of a medical institution
48.	Kali Linux құралдарын қолдана отырып, сымсыз желілердің осалдығын талдау.	Анализ уязвимостей беспроводных сетей с использованием инструментов Kali Linux.	Wireless network vulnerability analysis using Kali Linux tools.
49.	Зиянды бағдарламаларды динамикалық және статикалық талдау әдістерін зерттеу	Исследование методов динамического и статического анализа вредоносных программ	Research of methods dynamic and static analysis of malware
50.	«Kali Linux құралдарын қолдану арқылы осалдылықтарға талдау» электрондық оқу құралын әзірлеу	Разработка электронного учебного пособия «Анализ уязвимостей с использованием инструментов Kali Linux»	Development of an electronic tutorial "Vulnerability analysis using Kali Linux tools"
51.	Программалық қамтама осалдықтары негізінде эксплойттар тудыратын киберқауіптерді зерттеу	Исследование киберугроз, вызванных эксплойтами на основе уязвимостей программного обеспечения	Investigating cyberthreats caused by exploits based on software vulnerabilities
52.	Қауіпсіз Oracle деректер базасын Erwin-де жобалау, енгізу және басқару.	Проектирование, реализация и администрирование безопасной базы данных Oracle в Erwin	Design, implement and manage a secure Oracle database in Erwin.
53.	Linux ОЖ ядросының қауіпсіздігін дедуктивті верификациялау	Дедуктивная верификация безопасности ядра ОС Linux	Deductive verification of the security of the Linux OS kernel

54.	Жады дампын цифрлық криминалистикалық талдау құралдарын зерттеу	Исследование инструментов цифрового криминалистического анализа дампа памяти	Investigation of tools of digital forensic analysis of memory dump
55.	Linux ОЖ-нің қол жеткізуді басқару механизмін модельдеу	Моделирование механизма управления доступом ОС Linux	Modeling access control mechanism of the Linux OS
56.	Анонимділікті қамтамасыз ету әдістері мен құралдары және желідегі бақылаудан қорғау, сандық іздерді тазарту	Методы и средства обеспечения анонимности и защиты от отслеживания в сети, очистка цифрового следа	Methods and means of ensuring anonymity and network tracking protection, clearing the digital footprint
57.	Ақпараттық қауіпсіздікті қамтамасыз етуде DLP жүйелерін қолдану	Использование DLP-систем в обеспечении информационной безопасности	The use of DLP systems in ensuring information security
58.	Ену - тестілеу көмегімен желі қызметтері мен қосымшалар осалдықтарын зерттеу	Исследование уязвимостей сетевых служб и приложений с помощью тестирования на проникновение	Investigation of vulnerabilities of network services and applications using penetration testing
59.	Kali Linux операциялық жүйесін қолдана отырып фишинг шабуыл жүргізу және қауіпсіздікті қамтамасыз ету шаралары	Фишинговые атаки и меры безопасности с использованием операционной системы Kali Linux	Phishing attacks and security measures using the Kali Linux operating system
60.	Веб-қосымшалардың қауіпсіздігін қамтамасыз ету әдістері	Методы обеспечения безопасности web-приложения	The methods of ensuring the security of a web application
61.	KALI LINUX құралымен заманауи кибершабуылдарды іске асыру және алдын-алу шаралары	Реализация современных кибератак с помощью KALI LINUX и рекомендации по предотвращению	Implementation of modern cyber attacks using KALI LINUX and recommendations for prevention
62.	Стеганография жүйесін құру және жүйе беріктігін арттыру мәселелерін зерттеу	Разработка стеганографической системы и исследование вопросов повышения стойкости системы	Development of a steganographic system and research into the issues of increasing the resilience of the system

63.	Цифрлық дәлелдемелерді анықтау үшін цифрлық форензиканы қолдану	Использование цифровой форензики для выявления цифровых доказательств	Using digital forensics to identify digital evidence
64.	Банктегі ақпараттық қауіпсіздікті жетілдірудің әдістері	Методы совершенствования информационной безопасности в банке	Methods of improving information security in the bank
65.	Құпия ақпаратты тарату кезінде стеганографияның қолданылуын зерттеу	Исследование применения стеганографии при передаче конфиденциальной информации	Investigation of the use of steganography in the transmission of confidential information
66.	SQL инъекция түріндегі шабуылдардан веб-сайттардың осалдығын іздеу	Поиск уязвимости WEB-сайтов от атак типа SQL- инъекции	Search for vulnerability of WEB sites from SQL injection attacks
67.	Threat Hunting құралдары көмегімен қауіптерді белсенді іздеу және анықтау	Проактивный поиск и обнаружение угроз с помощью инструментов Threat Hunting	Proactive search and detection of threats using Threat Hunting tools
68.	Ddos-шабуылдарды анықтау үшін машиналық оқытудың қолданылуын зерттеу	Исследование применимости машинного обучения для определения ddos атак	Study of the applicability of machine learning to detect ddos attacks
69.	Ұйымдағы ақпараттық желі қолданушыларының жеке деректерін қорғаудың әдістері	Способы защиты персональных данных пользователей информационной сети в организации	Ways to protect personal data of information network users in an organization
70.	Желілік шабуылды модельдеуге негізделген веб-сайт қауіпсіздігін талдау	Анализ защищённости веб-сайтов на основе моделирования сетевых атак	Analysis of site security based on network attack modeling
71.	Аспаптық тестілеу әдістеріне негізделген web-қосымшалардың осалдықтарын зерттеу	Исследование уязвимостей web-приложений на основе методов инструментального тестирования	Exploring web-application vulnerabilities based on instrumental testing methods

72.	Зиянды және күдікті файлдарды анықтау үшін оқшауланған ортаны (құмсалғыш) талдау	Анализ изолированной среды (песочницы) для обнаружения вредоносных и подозрительных файлов	Analysis of an isolated environment (sandbox) to detect malicious and suspicious files
73.	Kali Linux құралдары арқылы WPA/WPA2 желілерінің шабуылдары мен қорғаныс әдістерін зерттеу	Исследование атак и способов защиты сетей WPA/WPA2 с использованием инструментария Kali Linux	A study of attacks and ways to protect WPA/WPA2 networks using Kali Linux tools
74.	Маңызды қорғау объектілеріндегі ақпараттық қауіпсіздік жүйелерін тестілеу және сынау нәтижелерінің дұрыстығын арттыру әдістері	Методы повышения достоверности результатов тестирования и испытаний систем информационной безопасности на критически важных объектах защиты	Methods to improve the reliability of the results of testing and evaluating information security systems at critical protection targets
75.	Әлеуметтік инженерия әдістері арқылы ашық ақпарат көздерінен жеке деректерді жинақтау	Сбор персональных данных из открытых источников посредством применения методов социальной инженерии	Collection of personal data from open sources through the social engineering methods
76.	Ұйымдардағы тұлғалардың жеке мәліметтерін программалық және құқықтық қорғау	Программно-правовая защита персональных данных физических лиц в организациях	Program-legal protection of personal data of individuals in organizations
77.	Passive optical network қорғалған желісін жобалау	Проектирование защищенной сети Passive optical network	Design of a secure Passive optical network
78.	Стандартты WEP ағынды шифрлау протоколын шабуылдардан қорғау әдістерін зерттеу	Исследование методов защиты стандартного протокола потокового шифрования WEP от атак	A study of methods for defending against attacks on the standard WEP streaming encryption protocol
79.	Мобильді робототехникалық кешендердің радиоарналарындағы ақпаратты қорғау әдістерін зерттеу	Исследование методов защиты информации в радиоканалах мобильных робототехнических комплексов	A study of methods information security methods in radiochannels of mobile robotic complexes

80.	Қашықтықтан банктік қызмет көрсету жүйесін талдау және мәліметтерді қорғау	Анализ системы дистанционного банковского обслуживания и защиты данных	Analysis of the system of remote banking services and protection of data
81.	Веб-қосымшалардағы авторизацияның кемшіліктері	Недостатки авторизации в веб приложениях	Disadvantages of authorization in web applications
82.	«SMART HOUSE» жүйесіндегі ақпараттық қауіпсіздік қатерлерін талдау»	«Анализ угроз информационной безопасности в системе «SMART HOUSE»	«Analysis of information security threats in the SMART HOUSE system»
83.	C++ программалау тілінің осалдықтары және оларды жою тәсілдері	Уязвимости языка программирования C++ и методы их устранения	Programming language vulnerabilities C++ and their methods are eliminated
84.	Ақпараттық қауіпсіздік саласындағы инциденттерді тергеу құралдарын салыстырмалы талдау	Сравнительный анализ инструментов расследования инцидентов в области информационной безопасности	Comparative analysis of information security incident investigation tools
85.	MySQL-де деректер қауіпсіздігін қамтамасыз ету әдістері мен құралдары	Методы и средства обеспечения безопасности данных в MySQL	Data security methods and tools in MySQL
86.	Фейстель желісіне негізделген блоктық шифрлардың сызықтық криптоанализі	Линейный криптоанализ блочных шифров, основанных на сети Фейстеля	Linear Cryptanalysis of Block Ciphers Based on the Feistel Network
87.	Маңызды инфрақұрылым объектілеріндегі кибертеррорлық қауіптерді зерттеу	Исследование угроз кибертерроризма на объекты критической инфраструктуры	Research of threats of cyberterrorism on objects of critical infrastructure
88.	Ақпараттық қауіпсіздік қауіптерін ерте анықтау және оларға қарсы әрекет ету құралдарын талдау және әдістемесін әзірлеу	Разработка методики и анализ средств раннего выявления и противодействия угрозам информационной безопасности	Development of a methodology and analysis of means for early detection and counteraction to information security threats
89.	Telegram API көмегімен екі факторлы аутентификацияны ұйымдастыру	Организация двухфакторной аутентификации с использованием Telegram Api	Organization of two-factor authentication using Telegram API

90.	Компьютерлік желілер аясындағы делдалдық шабуылдар: алдын алу, анықтау және қарсы әрекет ету	Атаки посредника в компьютерных сетях: предотвращение, обнаружение и противодействие	Preventing, Detecting, and Countering Computer Networks MITM Attacks
91.	Мемлекеттік құрылымдардың ашық ақпараттық жүйелерінде деректерді қорғауды қамтамасыз ету тәсілдерін жетілдіру	Совершенствование подходов к обеспечению защиты данных в открытых информационных системах государственных структур	Improving approaches to ensuring data protection in open information systems of state structures
92.	Компьютерлік жүйелердің қауіпсіздігін қамтамасыз етудегі виртуалдандыру технологияларының тиімділігін бағалау	Оценка эффективности технологий виртуализации в обеспечении безопасности компьютерных систем	Evaluation of the effectiveness of virtualization technologies in ensuring the security of computer systems
93.	Реляциялық емес деректер базаларының қауіпсіздігін қамтамасыз ету әдістері мен құралдары	Методы и средства обеспечения безопасности нереляционных баз данных	Methods and tools for securing non-relational databases
94.	Ақпараттық желілік қауіпсіздікті қамтамасыз етудің интеллектуалды-бейімделу әдістері	Интеллектуально- адаптивные методы обеспечения безопасности информационных сетей	Intelligent and adaptive methods for ensuring the security of information networks
95.	Windows және Linux вирус жұқтырған жүйелерді зерттеуге арналған цифрлық криминалистикалық сараптамасының әдістері мен құралдарын зерттеу	Исследование методов и инструментов цифровой криминалистической экспертизы для исследования зараженных Windows и Linux систем	Investigation methods and digital forensics tools for investigating infected Windows and Linux systems
96.	QUIC протоколы негізінде DDoS шабуылынан қорғау әдістері мен жүйелері.	Методы и системы защиты от атаки типа "отказ в обслуживании" (DDoS) на основе протокола QUIC	Methods and systems for protection against «denial of service»(DDoS) type attack based on the QUIC protocol
97.	Маркирленген тауарларды жеткізуді қадағалау процесіне блокчейн технологиясын енгізу	Внедрение технологии блокчейн в процесс отслеживания поставок маркированных товаров	Implementation of blockchain technology in the process of tracking the supply of labeled goods
98.	Протекторлар мен ораушыларда қолданылатын анти-талдау техникаларын қолданбай өту әдістері	Методы обхода техник анти-анализа, применяемых в протекторах и упаковщиках	Methods for bypassing anti-analysis techniques used by protectors and packers

99.	Рұқсатсыз кіруді болдырмау үшін VPN технологиясын қолдану арқылы желілік қауіпсіздікті қамтамасыз ету	Обеспечение сетевой безопасности с использованием технологии VPN для предотвращения несанкционированного доступа	Network security with VPN technology to prevent unauthorized access
100.	Ашық ақпарат көздеріне негізделген Threat Intelligence жүйесін құру	Создание системы Threat Intelligence на основе открытых источников информации	Creation of a Threat Intelligence system based on open sources of information.
101.	Web-қосымшалардың ақпараттық қауіпсіздігін қамтамасыз ету әдістерін жүзеге асыру	Реализация методов обеспечения информационной безопасности Web-приложений	Implementation of methods for ensuring information security of Web-applications
102.	Ашық Интернет көздерінен ақпаратты жинау және талдау үшін OSINT құралдарын зерттеу	Исследование OSINT инструментов для сбора и анализа информации из открытых источников Интернета	Study of OSINT tools for collecting and analyzing information from open Internet sources
103.	Жедел жадыны криминалистикалық талдау шеңберінде автоматты түрде орындалатын файлдарды зерттеуді автоматтандыру	Автоматизация исследования автозапускаемых исполняемых файлов в рамках криминалистического анализа оперативной памяти	Automating the study of autorun executable files as part of the forensic analysis of RAM
104.	Өндіруші компаниялардың ақпараттық қауіпсіздік жүйесінің математикалық моделін әзірлеу және талдау	Разработка и анализ математической модели системы информационной безопасности добывающих компаний	Development and analysis of a mathematical model of the information security system of mining companies
105.	Әлеуметтік инженерлік шабуылдарды және оларға қарсы тұру жолдарын зерттеу	Исследование атак социальной инженерии и способов противодействия им	Study of social engineering attacks and ways to counter them
106.	Ақпараттық қауіпсіздік оқиғасына жауап ретінде дискілердің бейнелері бойынша автоматты түрде орындалатын файлдарды зерттеуді автоматтандыру	Автоматизация исследования автозапускаемых исполняемых файлов при изучении образов дисков в рамках реагирования на инцидент информационной безопасности	Automating the examination of autorun executable files when examining disk images as part of an information security incident response
107.	Корпоративтік желіде Open Source SIEM жүйесін қолдана отырып қауіпсіздікті басқару	Управление безопасностью с применением системы Open Source SIEM в корпоративной сети	Security management using the Open Source SIEM system in the enterprise network

108	Несиелік ұйымдардағы ақпараттық қауіпсіздік қатерлерін зерттеу	Исследование угроз безопасности информации в кредитных организациях	Study of information security threats in credit institutions
109	Кәсіпорындардың P2P желісіне бағытталған DDoS шабуылдарын анықтау және қорғау әдістерін талдау	Анализ методов обнаружения и защиты от DDoS атак на P2P сети предприятий	Analysis of methods to detect and defend against DDoS attacks on enterprise P2P networks
110	Кәсіпорындағы ақпараттық қауіпсіздік тәуекелдерін бағалау үшін құжаттаманы әзірлеу	Разработка документации для оценки рисков информационной безопасности на предприятии	Development of documentation for assessing information security risks in the enterprise
111	ТЖ кәсіпорнында пайдаланушыларды қорғау бойынша ақпараттық қауіпсіздікті ұйымдастыру	Организация информационной безопасности по защите пользователей на ЖД предприятии	Organization of information security to protect users at the railway enterprise
112	ТЖ кәсіпорнында ақпараттық жүйелерді ұйымдастыру және қорғау	Организация и защита информационных систем на ЖД предприятии	Organization and protection of information systems at the railway enterprise
113	Күзет компаниясы үшін жеке деректерді қорғаудың қауіпсіздік саясатын әзірлеу	Разработка политики безопасности по защите персональных данных для охранной организации	Development of a security policy for the protection of personal data for a security organization
114	Web-қосымшалардың қорғалғандығын талдау үшін шабуылдарды моделдеу	Моделирование атак для анализа защищенности Web-приложений	Attack modeling for Web-application security analysis
115	Кәсіпорын бойынша оқиғаларға жауап беру	Реагирование на инциденты в масштабах предприятия	Enterprise-wide incident response
116	OSINT заманауи технологиясы негізінде .kz домендік аймағындағы осалдықтарды автоматты іздеу үшін программалық қамтаманы әзірлеу	Разработка программного обеспечения для автоматизированного поиска уязвимостей в доменной зоне .kz на основе современных технологий OSINT	Development of software for automated search for vulnerabilities in the .kz domain zone based on modern OSINT technologies
117	Антибуллингтік интернет порталы	Антибуллинговый Интернет портал	Anti-bullying Internet portal

118	Шабуылдаушылардың іс-әрекеттерінің модельдері мен сценарийлерінің ақпараттық қауіпсіздік тәуекелдерін талдау әдістеріне әсері	Влияние моделей и сценариев действий злоумышленников на методы анализа рисков информационной безопасности	Influence of models and scenarios of malicious actions on methods of information security risk analysis
119	Зиянды программалардың Sandbox жүйесін айналып өту әдістерін талдау	Анализ методов обхода песочниц вредоносными ПО	Analysis of methods for bypassing sandboxes by malware
120	Құрылыс ұйымдарының ақпараттық қауіпсіздік саясатын әзірлеу	Разработка политики информационной безопасности для строительных организаций	Development of an information security policy for construction organizations
121	ТЖ кәсіпорнында желілік инфрақұрылымның ақпараттық қауіпсіздігінің аудитін ұйымдастыру	Организация аудита информационной безопасности сетевой инфраструктуры на ЖД предприятии	Organization of an audit of information security of the network infrastructure at the railway enterprise
122	Ақпараттық қауіпсіздік стандарттары бойынша ТЖ кәсіпорны үшін бизнес моделін әзірлеу	Разработка бизнес модели для ЖД предприятия по стандартам информационной безопасности	Development of a business model for a railway company according to information security standards
123	Дискідегі кескіндерді криминалистикалық сараптау кезінде орындалатын файлдарды іске қосу тарихын зерттеуді автоматтандыру	Автоматизация исследования истории запущенных исполняемых файлов при криминалистическом изучении образов дисков.	Analysis of the history of running executable files during forensic examination of disk images
124	Зиянкестердің бақыланатын ортада зиянды объектілерді орындауын анықтау әдістері және оларға қарсы әрекет ету	Методы детектирования злоумышленниками исполнения вредоносных объектов в контролируемом окружении и противодействие им	Methods for detecting the execution of malicious objects in a controlled environment by intruders and counteracting them
125	желілердің қауіпсіздігін қамтамасыз ету әдістері	Методы обеспечения безопасности в сетях	Methods of ensuring the security of networks

126	Деректер қорын алу үшін SQL инъекциясын зерттеу	Исследование SQL-инъекции для извлечения информации в базе данных	Investigating SQL Injection to Extract Information in a Database
127	Әлеуметтік желілердегі ақпаратты қорғау әдістері	Методы защиты информации в социальных сетях	Methods for protecting information in social networks
128	Операциялық жүйелерінің толық қауіпсіздігі	Полная безопасность операционных систем	Complete security of operating systems
129	Веб-қосымшалардағы қауіпсіздікке қатер төндіретін жарнамалық ақпаратты блоктауға арналған программаны әзірлеу	Разработка программы для блокировки рекламной информации, представляющей угрозу безопасности в веб-приложениях	Development of a program for blocking advertising information that poses a security threat in web applications
130	Лог файлдарының көмегімен web қосымшаларды қорғау	Защита web приложение с помощью лог-файлов	Protecting web applications with log files
131	Веб-қосымшаларға шабуыл жасауға арналған құралдар	Инструменты предназначенных для атаки веб-приложений.	Tools designed to attack web applications
132	Ақпараттық қауіпсіздік анықтау үшін Wireshark арқылы желілік трафикті талдау	Анализ сетевого трафика посредством Wireshark для определения информационной безопасности	Analysis of network traffic through Wireshark to identify information security
133	Ақпараттық қауіпсіздікте стеганографияны қолдану	Применение стеганографии в информационной безопасности	Application of steganography in information security
134	OSI моделінің желілік деңгейлерінде маршрутизаторлар қауіпсіздігін қамтамасыз ету	Обеспечение безопасности маршрутизаторов на сетевом уровнях модели OSI	Securing Routers at the Network Layers of the OSI Model

135	WEB-беттерді скриптингтен қорғау	Защита WEB-страниц от скриптинга	Protecting WEB-pages from scripting
136	Ақпараттық технологиялар саласындағы мекемелер үшін ақпараттық қауіпсіздікті қамтамасыз ету	Обеспечения информационной безопасности для организации в сфере информационных технологий	Ensuring information security for an organization in the field of information technology
137	Кәсіпорында IT инфрақұрылымын дамыту бойынша стандартты әзірлеу	Разработка стандарта по развитию IT инфраструктуры на предприятии	Development of standard for the development of IT infrastructure at the enterprise
138	Нейро-бұлдыр желілерді қолдана отырып, ақпараттық қауіпсіздік жүйелеріне арналған құралдар құру	Создания инструментария для систем информационной безопасности с использованием нейро-нечётких сетей	Creation of tools for information security systems using neuro-fuzzy networks
139	Кәсіпорнын қорғаудың программалық жүйесін әзірлеу	Разработка программной системы защиты на предприятии	Development of a software protection system
140	Клиент желісінің топологиясындағы осалдықтар	Уязвимости в топологии сети клиента	Vulnerability in the client's network topology
141	Желілік байланыс жағдайында жеке тұлғаның ақпараттық қауіпсіздігі	Информационная безопасность личности в условиях сетевой коммуникации	Information security of the individual in the conditions of network communication on the example
142	Мобильді пайдаланушылардың VPN сеанстарының ағып кетуінен қорғау құралдарын зерттеу	Исследование средств защиты от утечек сеансов VPN мобильных пользователей	Research of means of protection against leakage of VPN sessions of mobile users
143	Kali Linux операциялық жүйесінің құралдары арқылы тестілеу жүргізу	Проведение тестирования на посредством инструментов операционной системы Kali Linux	Conducting testing based on the tools of the Kali Linux system

144	Nikto website vulnerabilities scanner көмегімен осалдықтарды анықтау	Обнаружение уязвимостей с помощью сканера уязвимостей сайта Nikto	Finding Vulnerabilities with Nikto's Vulnerability Scanner
145	Автоматтандырылған кәсіпорын жүйесінде ақпаратты фишингтен қорғау әдістерін әзірлеу	Разработка методики защиты информации от целевого фишинга в автоматизированной системе предприятия	Development of methods for protecting information from spear phishing in an automated enterprise system
146	Кәсіпорындағы ақпараттық жүйелердің ақпараттық қауіпсіздігінің аудиті	Аудит информационной безопасности информационных систем на предприятии	Information security audit of information systems at the enterprise
147	PostgreSQL жүйесінде деректерді қорғау әдістері	Методы обеспечения безопасности данных в PostgreSQL	PostgreSQL data security methods
148	Зиянды программалық қамтаманы жедел жад ішінде анықтау әдістері	Методы обнаружение вредоносного программного обеспечения в оперативной памяти	Methods for detecting malware in RAM
149	Security information and event management жүйесін қолдана отырып, ақпараттық қауіпсіздікті қамтамасыз ету әдістері	Методы обеспечения информационной безопасности с использованием системы Security information and event management	Methods for ensuring information security using the Security information and event management system
150	Қауіпсіздік жүйесінде биометриялық деректерді пайдалану	Использование биометрических данных системы безопасности	Using biometric security data
151	Vpn технологиясын қолдана отырып кәсіпорынның корпоративтік желісінің қауіпсіздігі	безопасности корпоративной сети предприятия с применением технологии VPN	security of the corporate network of the enterprise using VPN technology
152	Корпоративтік желілерде ddos-шабуылдардан ақпаратты қорғау құралдары	Средств защиты информации в корпоративных сетях от ddos-атак	Means of protecting information in corporate networks from ddos attacks

153	Kali Linux құралдарының көмегімен Windows ОЖ-нің осалдығын талдау және енуін тестілеу	Анализ уязвимостей и тестирование на проникновение ОС Windows с помощью инструментов Kali Linux	Windows Vulnerability Analysis and Penetration Testing with Kali Linux Tools
154	Сымсыз желілерде ойын теориясын пайдалану	Использование теории игр в целях сетевой безопасности	Using Game Theory for Network Security
155	Интернет дүкеннің қауіпсіздігі	Безопасности интернет магазина	online store security systems
156	Веб-қосымшаларда сеанс құру	Создания сессии в веб приложениях	Creating a session in web applications
157	Ақпараттық қауіпсіздік мәселелерін шешудің алгоритмдерін құру	Разработка алгоритмов для решения задач защиты информации	Development algorithms for solving information protection tasks
158	Ақпараттық-коммуникациялық инфрақұрылымға шабуыл түрлері	Видов атак на информационно-коммуникационную инфраструктуру	Of types of attacks on information and communication infrastructure
159	Жұмыс орындарын кешенді қорғау	Комплексная защита рабочих мест	Comprehensive workplace protection
160	BGP-Hijack негізіндегі фишингтік шабуылдарды анықтау әдістері	Методы выявления фишинговых атак на базе BGP-Hijack	Of methods for detecting phishing attacks based on BGP-Hijack
161	Dll SideLoading осалдығын пайдалану арқылы жүйеге енгізілген зиянды программаларды іздеу	Поиска вредоносных закрепленных в системе с помощью эксплуатации уязвимости Dll SideLoading.	he search for malware embedded in the system by exploiting the Dll SideLoading vulnerability.

162	«Introduction to Cybersecurity» оқыту курсы	Учебный курс «Introduction to Cybersecurity»	Training course "Introduction to Cybersecurity"
163	Программалық қамтаманы әзірлеу кезінде ақпараттық қауіпсіздік (DevSecOps)	Информационной безопасности при разработке ПО (DevSecOps)	Information security in software development (DevSecOps)
164	Веб қосымшалардың аутентификациясындағы осалдықтар	Уязвимости аутентификации веб приложений	Vulnerabilities and weaknesses in web application
165	Биометриялық аутентификацияны пайдалана отырып, Интернет-дүкенінің қорғалған қосымшасын әзірлеу	Разработка защищенного приложения интернет-магазина с использованием биометрической аутентификации	Development of a secure application for online store using biometric authentication
166	КиберСтраж” кешенінің көмегімен ақпараттық қауіпсіздік	Информационной безопасности с помощью комплекса “КиберСтраж”	Information security using the CyberGuard complex
167	Ұйымдағы ақпараттық қауіпсіздік инциденттері	Инциденты информационной безопасности в организации	Information security incidents in the organization
168	HTTP серверін DDoS шабуылдарынан қорғау құралы	Средства защиты HTTP сервера от DDoS-атак	HTTP server protection tools from DDoS attacks
169	DDoS шабуылдарының әсерінен АҚЖ-не төнетін қауіпті жою әдісін жасау	Разработка способа устранения угроз к СИБ при действии DDoS -атак	Development of a method for eliminating threats to the NIS under the action of DDoS attacks
170	Деректер базасына төнетін қауіптер түрлері және олардан қорғану әдістері	Типы угроз для базы данных и методов защиты от них	Types of threats to the database and of methods of protection against them

171.	Медициналық мекеменің ақпараттық жүйесінің қауіпсіздік саясаты	Политики безопасности информационной системы медицинского учреждения	Information system security policies of a medical institution
172.	Kali Linux құралдарын қолдана отырып, сымсыз желілердің осалдығы	Уязвимостей беспроводных сетей с использованием инструментов Kali Linux.	Wireless network vulnerabilities using Kali Linux tools.
173.	Зиянды бағдарламаларды динамикалық және статикалық талдау	Динамического и статического анализа вредоносных программ	Dynamic and static malware analysis
174.	«Kali Linux құралдарын қолдану арқылы осалдылықтарға талдау» оқу құралы	Учебное пособия «Анализ уязвимостей с использованием инструментов Kali Linux»	Vulnerability Analysis Using Kali Linux Tools Tutorial
175.	Программалық қамтама осалдықтары негізінде эксплойттар тудыратын киберқауіптер	Киберугроз, вызванных эксплойтами на основе уязвимостей программного обеспечения	Cyberthreats caused by exploits based on software vulnerabilities
176.	Қауіпсіз Oracle деректер базасын Erwin-де жобалау	Проектирование безопасной базы данных Oracle в Erwin	Design a secure Oracle database in Erwin.
177.	Linux ОЖ қауіпсіздігін дедуктивті верификациялау	Дедуктивная верификация безопасности ОС Linux	Deductive Security Verification of Linux OS
178.	Жады дампын цифрлық криминалистикалық талдау	Цифрового криминалистического анализа дампа памяти	Digital forensic analysis of memory dump
179.	Linux ОЖ-нің қол жеткізуді басқару механизмі	Механизм управления доступом ОС Linux	Access control mechanism of the Linux OS

180	Анонимділікті қамтамасыз ету әдістері мен құралдары және желідегі бақылаудан қорғау	Методы и средства обеспечения анонимности и защиты от отслеживания в сети	Methods and means of ensuring anonymity and network tracking protection
181	Ақпараттық қауіпсіздікті қамтамасыз етуде DLP жүйелері	DLP-систем в обеспечении информационной безопасности	DLP systems in ensuring information security
182	Ену - тестілеу көмегімен желі қызметтері мен қосымшалар осалдықтары	Уязвимостей сетевых служб и приложений с помощью тестирования на проникновение	Vulnerabilities of network services and applications using penetration testing
183	Kali Linux операциялық жүйесін қолдана отырып фишинг шабуыл жүргізу және қауіпсіздікті қамтамасыз ету	Фишинговые атаки безопасности с использованием операционной системы Kali Linux	Security phishing attacks using the Kali Linux operating system
184	Веб-қосымшалардың қауіпсіздігін қамтамасыз ету	Обеспечения безопасности web-приложения	Ensuring the security of a web application
185	KALI LINUX құралымен заманауи кибершабуылдарды алдын-алу шаралары	Современных кибератак с помощью KALI LINUX и рекомендации по предотвращению	Modern cyber attacks using KALI LINUX and recommendations for prevention
186	Стеганография жүйесін құру және жүйе беріктігін арттыру мәселелері	Стеганографическое системы и исследование вопросов повышения стойкости системы	Steganographic systems and the study of issues of increasing the stability of the system
187	Ақпараттық қауіпсіздік жүйесін құрылымдау: әдістері, модельдері, аспаптық құралдары	Структурирование системы информационной безопасности: методы, модели, инструментальные средства	Structuring an information security system: methods, models, tools
188	Таратылған типтегі кәсіпорындардағы ақпараттық қауіпсіздік жүйесін оңтайландыру әдістері мен модельдері	Методы и модели оптимизации системы информационной безопасности на предприятиях распределенного типа	Methods and models of information security system optimization in distributed enterprises

189	Корпоративтік ақпараттық жүйенің ақпараттық қауіпсіздігін қамтамасыз етуді модельдеу	Моделирование обеспечения информационной безопасности корпоративной информационной системы	Modeling of information security of a corporate information system
190	Экономикалық ақпараттық жүйелердегі қауіпсіздікті қамтамасыз ету тиімділігін бағалау әдістемесі	Методология оценки эффективности обеспечения безопасности в экономических информационных системах	Methodology for assessing the effectiveness of security in economic information systems
191	Өнеркәсіптік кәсіпорындардың ақпараттық қауіпсіздігін қамтамасыз ету жүйесін дамыту	Развитие системы обеспечения информационной безопасности промышленных предприятий	Development of the information security system of industrial enterprises
192	Таратылған корпоративтік ақпараттық жүйедегі әкімшілік қауіпсіздік әдістері	Методы административной безопасности в распределенной корпоративной информационной системе	Methods of administrative security in a distributed corporate information system
193	Сенсорлық экран технологиялары мен виртуалды шындыққа негізделген адам-компьютерлік интерфейстердің қауіпсіздігін бағалау	Оценивание защищённости человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности	Assessment of the security of human-computer interfaces based on touch screen technologies and virtual reality
194	Уақыт қатарларын талдау негізінде киберфизикалық жүйелердің ақпараттық қауіптерден қорғалуын бағалау моделі мен әдісі	Модель и метод оценивания защищённости киберфизических систем от информационных угроз на основе анализа временных рядов ретроспективной, текущей и экспертной информации	A model and method for assessing the security of cyber-physical systems from information threats based on time series analysis
195	Ақпаратты білім беру желілерінде рұқсатсыз кіруден қорғау	Защита информации от несанкционированного доступа в образовательных сетях	Protection of information from unauthorized access in educational networks
196	Дербес деректерді өңдеудің ақпараттық жүйелерінің қауіпсіздігінің өзекті қатерлерін зерттеу үшін имитациялық	Разработка и реализация имитационных и математических моделей для исследования актуальных	Development and implementation of simulation and mathematical models for the study of current threats to the

	және математикалық модельдерді әзірлеу және іске асыру	угроз безопасности информационных систем обработки персональных данных	security of personal data processing information systems
197	Ретроспективті, ағымдағы және сараптамалық ақпарат негізінде аппараттық-бағдарламалық кешендердің функционалдық қауіпсіздігін бағалау	Оценка функциональной безопасности аппаратно-программных комплексов на основе	Functional safety assessment of hardware and software complexes based on retrospective, current and expert information
198	Қорғалған ақпараттық жүйенің қауіпсіздік тәуекелдерін талдау және басқару әдісі	Метод анализа и управления рисками безопасности защищенной информационной системы	Method of analysis and management of security risks of a protected information system
199	Қол жеткізуді басқару және басқару модельдерін және қауіпсіздік саясатын модельдеу әдістерін талдау.	Анализ моделей контроля и управления доступом и методов моделирования политик безопасности	Analysis of access control and management models and methods for modeling security policies.
200	Дербес деректердің ақпараттық жүйелеріндегі ақпараттық қауіпсіздіктің өзекті қатерлерін айқындау әдістемесі мен алгоритмдері	Методика и алгоритмы определения актуальных угроз информационной безопасности в информационных системах персональных данных	Methodology and algorithms for determining current threats to information security in personal data information systems
201	Автоматтандырылған жүйелердегі ақпараттық қауіпсіздік тәуекелдерін динамикалық итеративті бағалау	Динамическая итеративная оценка рисков информационной безопасности в автоматизированных системах	Dynamic iterative assessment of information security risks in automated systems
202	Бағдарламалық жүйе және компьютерлік желілердегі ақпараттық қауіпсіздікке төнетін қатерлерді анықтау тәсілі	Программная система и способ выявления угроз информационной безопасности в компьютерных сетях	Software system and method for identifying information security threats in computer networks
203	Күрделі ұйымдық жүйелердегі ақпараттық қауіпсіздікті қамтамасыз етудің желілік модельдері мен әдістері	Сетевые модели и методы обеспечения информационной безопасности в сложных организационных системах	Network models and methods of information security in complex organizational systems
204	Дербес деректердің ақпараттық жүйесінің қауіпсіздігіне аудит жүргізу кезінде ақпараттық тәуекелдерді талдаудың	Модели и алгоритмы анализа информационных рисков при проведении аудита безопасности	Models and algorithms for the analysis of information risks during the audit of the security of the personal data

	модельдері мен алгоритмдері	информационной системы персональных данных	information system
205	Сыни жүйелерді басқарудың автоматтандырылған жүйелерінің ақпараттық қауіпсіздігін бағалау және қамтамасыз ету әдістері мен модельдері	Методы и модели оценки и обеспечения информационной безопасности автоматизированных систем управления критическими системами	Methods and models for assessing and ensuring information security of automated critical systems management systems
206	Тематикалық интернет-ресурстардың деректерін талдау негізінде ақпараттық қауіпсіздіктің қауіптері мен осалдықтарын болжаудың ақпараттық-талдамалық жүйесі	Информационно-аналитическая система прогнозирования угроз и уязвимостей информационной безопасности на основе анализа данных тематических интернет-ресурсов	Information and analytical system for forecasting threats and vulnerabilities of information security based on data analysis of thematic Internet resources
207	Кәсіпорын үшін ақпаратты қорғаудың бағдарламалық-аппараттық жүйесін әзірлеу	Разработка программно-аппаратной системы защиты информации для предприятия	Development of a hardware and software information protection system for the enterprise
208	Кәсіпорында ақпаратты қорғау жүйесін жобалау және енгізу	Проектирование и внедрение системы защиты информации на предприятии	Design and implementation of the information security system at the enterprise
209	Корпоративтік ақпараттық ортадағы қауіпсіздікті басқару	Управление безопасностью в корпоративной информационной среде	Security management in the corporate information environment
210	Объектінің ақпараттық қауіпсіздігінің жай-күйін мониторингілеу	Мониторинг состояния информационной безопасности объекта	Monitoring of the information security status of the facility
211	Кәсіпорынға қорғалған құжат айналымын ұйымдастыру	Организация защищённого документооборота на предприятие	Organization of secure document flow to the enterprise

212	Маңызды ақпараттық инфрақұрылымның ақпараттық қауіпсіздігінің тәуекелдерін талдау әдістемесін әзірлеу	Разработка методики анализа рисков информационной безопасности критической информационной инфраструктуры	Development of a methodology for analyzing information security risks of critical information infrastructure
213	Кәсіпорынның қорғалған есептеу желісінің жобасын әзірлеу	Разработка проекта защищенной вычислительной сети предприятия	Development of a project for a secure enterprise computer network
214	Кәсіпорындағы қолжетімділікті бақылау жүйесін жаңғырту жобасын әзірлеу	Разработка проекта модернизации системы контроля доступа на предприятии	Development of a project to modernize the access control system at the enterprise
215	Корпоративтік компьютерлік желінің ақпараттық қауіпсіздік жүйесін құру	Построение системы информационной безопасности корпоративной компьютерной сети	Building an information security system for a corporate computer network
216	Брандмауэрлерді жергілікті компьютерлік желіні қорғау құралы ретінде пайдалану	Использование межсетевых экранов как средств защиты локальной компьютерной сети	The use of firewalls as a means of protecting a local computer network
217	ақпаратты қорғау жүйесінің қауіпсіздігін талдау	анализ защищенности системы защиты информации	analysis of the security of the information security system
218	Веб сайтқа кіруді анықтау әдістерін әзірлеу	Разработка методов обнаружения вторжений на веб сайт	Development of methods for detecting website intrusions
219	Желілік платформалардың үлгілік қатерлеріне мониторинг және ден қоюдың автоматты жүйесін әзірлеу	Разработка автоматическо системы мониторинга и реагирования на типовые угрозы сетевых платформ	Development of an automated system for monitoring and responding to typical threats of network platforms

220	Ықтимал қауіпті вирустық қосымшаларды талдау әдістемесі	Методология анализа потенциально опасных вирусных приложений	Methodology for analyzing potentially dangerous virus applications
221	Инсайдерлік қызметтен болатын тәуекелдерді бағалаудың бағдарламалық кешенін әзірлеу	Разработка программного комплекса оценки рисков от инсайдерской деятельности	Development of a software package for assessing risks from insider activity
222	Қол жеткізу құқықтарының аражігін ажырату арқылы қол жетімсіздікті ақпаратпен қамтамасыз ету	Обеспечение информационной безоастьнлсть с помощью разграничение прав доступа	Providing information security with the help of access rights differentiation
223	Қорғалған корпоративтік желіні ұйымдастыру	Организация защищённой корпоративной сети	Organization of a secure corporate network
224	Ықтимал қауіпті қосымшаларды талдау әдістемесі	Методология анализа потенциально опасных приложений	Methodology for analyzing potentially dangerous applications
225	Биометриялық сәйкестендіру жүйесін әзірлеу	Разработка системы биометрической идентификации	Development of a biometric identification
226	желіні қызмет көрсетуден бас тартуға таратылған шабуылдан қорғау үшін шешім әзірлеу	разработка решения для защиты сети от распределенной атаки на отказ в обслуживании	system development of a solution to protect the network from a distributed denial of service attack
227	Кәсіпорындағы инсайдерлік белсенділікті бағалаудың ақпараттық-аналитикалық жүйесінің моделін әзірлеу	Разработка модели информационно-аналитической системы оценки инсайдерской активности на предприятии	Development of a model of an information and analytical system for assessing insider activity in an enterprise
228	Зиянды әрекеттерді анықтау және зерттеу үшін компьютерлік криминалистика әдістерін қолдану	Применение методов компьютерной криминалистики для обнаружения и изучения вредоносной активности	Application of computer forensics methods to detect and study malicious activity

229	Қосымшаның және сайттың ақпараттық қауіпсіздігін қамтамасыз ету жүйесін әзірлеу	Разработка системы обеспечения информационной безопасности приложения и сайта	Development of an application and website information security system
230	Компанияның виртуалды инфрақұрылымын қорғау жүйесін әзірлеу	Разработка системы защиты виртуальной инфраструктуры компании	Development of the company's virtual infrastructure protection system
231	Стеганография арқылы ақпаратты жасырудың заманауи әдістерін талдау	Анализ современных методов скрывтия информации средствами стеганографии	Analysis of modern methods of hiding information by means of steganography
232	Банкомат желісінің криптографиялық қорғаныс жүйесін зерттеу	Исследование системы криптографической защиты банкоматной сети	Investigation of the cryptographic protection system of the ATM network
233	Ықтимал зиянды қосымшаларды талдау әдістемесі	Методика анализа потенциально вредоносных приложений	Methodology for analyzing potentially malicious applications
234	Кәсіпорында ақпараттық қауіпсіздікті басқару жүйесін енгізу	Внедрение системы управления информационной безопасности на предприятии	Implementation of the information security management system at the enterprise
235	Шабуылдардан және деректердің бұзылуынан қорғау үшін дербес жұмыс орнын дайындау әдістемесін әзірлеу	Разработка методики подготовки автономного рабочего места для защиты от атак и утечки данных	Development of a methodology for preparing an autonomous workplace to protect against attacks and data leakage
236	Электрондық құжат айналымын қорғау бойынша ұсыныстар әзірлеу	Разработка предложений по защите электронного документооборота	Development of proposals for the protection of electronic document flow
237	Әлеуметтік желілер: жеке деректерді қорғау	Социальные сети: защита о персональных данных	Social networks: protection of personal data

238	Ақпаратты рұқсатсыз кіруден қорғау құралдарын қолдану технологиясы	Технология применения средств защиты информации от несанкционированного доступа	Technology for the use of information protection tools against unauthorized access
239	Нейрондық желіге негізделген төмен қарқынды DDoS шабуылдарын анықтау әдісі	Метод обнаружения низкоинтенсивных DDoS-атак на основе нейронной сети	A method for detecting low-intensity DDoS attacks based on a neural network
240	Ақпараттық қауіпсіздікте бұлтты технологияларды қолдану	Применение облачных технологий в информационной безопасности	Application of cloud technologies in information security
241	Ақпараттық жүйелер мен технологиялардың қауіпсіздігі мәселелері	Проблемы безопасности информационных систем и технологий	Security problems of information systems and technologies
242	Bluetooth-Защита осал арналарды пайдаланып шабуылдардан қорғау	Защита Bluetooth от атак с использованием уязвимых каналов	Protecting Bluetooth from attacks using vulnerable channels
243	Қауіпсіздік критерийлері бойынша компьютерлік желілерге арналған IP хаттамаларын зерттеу	Исследование IP протоколов для компьютерных сетей по критериям безопасности	Research of IP protocols for computer networks by security criteria
244	Ақпараттық-коммуникациялық инфрақұрылымның қауіпсіздік деңгейін есептеу	Расчет уровня безопасности информационно-коммуникационной инфраструктуры	Calculation of the security level of information and communication infrastructure
245	Осалдықтар Дерекқоры бойынша перспективалық қатерлерді талдау және шабуылдарды дамыту сервисі	Сервис анализа перспективных угроз и развития атак по базам данных уязвимостей	Service for the analysis of promising threats and the development of attacks on vulnerability databases
246	Ұйымның ақпараттық ресурстарына қашықтан қорғалған қолжетімділікті қамтамасыз ететін құралдар кешенін әзірлеу	Разработка комплекса средств,обеспечивающих удаленный защищенный доступ к информационным ресурсам	Development of a set of tools that provide remote secure access to information resources of the organization

		организации	
247	Компьютерлік желіге шабуылдарды анықтаудың заманауи құралдарын талдау	Анализ современных средств обнаружения атак на компьютерную сеть	Analysis of modern means of detecting attacks on a computer network
248	Веб-ресурстарды кибершабуылдан қорғауды бағалау	Оценка защиты веб-ресурсов от кибератак	Evaluation of the protection of web resources from cyber attacks