Тематика дипломных работ
по специальности 5В100200-«Системы информационной безопасности»
на 2021-2022 учебный год

1. Технологии противодействия хакерским утилитам и вредоносным программам
2. Исследование уязвимостей процесса аутентификации в веб приложениях и методы их устранения
3. Защита информации с помощью Firebase Cloud Storage
4. Разработка канала для защищенной передачи сообщений в локальной сети
5. Исследование сохранения данных на стороне клиента
6. Реализация метода криптокодирования
7. Двухфакторная аутентификация с использованием Telegram Api
8. Исследование инструментов Java для поддержки инфраструктуры открытых ключей
9. Уязвимости и методы безопасности SS7 сетей
10. Защита персональных данных и обеспечение информационной безопасности в сетях телемедицины
11. Обеспечение информационной безопасности платежных систем
12. Анализ передачи данных в rest api
13. Методы обеспечения безопасности веб-сайтов
14. Многофакторная аутентификация в облачных вычислениях
15. Исследование методов тестирования на проникновение с помощью языка Python
16. Компьютерные вирусы и принципы работы антивирусных программ
17. Разработка фреймворка автоматизированного тестирования веб-приложений
18. Исследование применения конечных автоматов Post-Initial для построения криптосистем
19. Разработка методов для защиты от кибератак
20. Технологии сниффинга сетевого трафика
21. Методы и критерии оценки адекватности модели информационной безопасности систем защиты информации
22. Исследование стандартов безопасного кодирования CERT Oracle для Java
23. Программно-определяемые уязвимости сетей
24. Исследование методов динамического анализа вредоносных программ
25. Разработка защищенного web-приложения «Цифровая площадка для студентов и работодателей»
26. Разработка системы информационной безопасности локальной вычислительной сети SEO-компании
27. Исследование методов безопасности протоколов ssl
28. Методы и методики оценки качества систем информационной безопасности
29. Методы и способы защиты от компьютерных преступлений
30. Исследование методов управление безопасностью мобильных абонентских устройств в корпоративных сетях
31. Разработка безопасной корпоративной сети с использованием технологии VPN
32. Исследование мобильных приложений, используемых для мониторинга окружающей среды и здоровья
33. Исследование виртуальных защищенных сетей на базе протокола IpSec и IKE
34. Организация защиты персональных данных в условиях реализации вирусных атак

35. Разработка программной реализации криптографического протокола голосования
36. Исследование методов масштабирования и оптимизации баз данных информационных систем
37. Разработка программной реализации криптографического протокола для зашифрования сообщений на заданное время
38. Исследование алгоритмов стеганографии в графических файлах
39. Исследование распределенной системы обнаружения и предотвращения атак типа ARP-spoofing
40. Исследование методов статического анализа вредоносных программ
41. Система контроля и управления доступом
42. Исследование методов разработки комплексов антивирусной безопасности в компании
43. Расследование инцидентов на основе методов сетевой форензики
44. Методы защиты от Web-скрапинга
45. Исследование использования методов биометрической аутентификации в мобильных устройствах
46. Автоматизация процесса реагирования на инциденты информационной безопасности на основе решений класса Threat Intelligence Platform
47. Методы криминалистической экспертизы операционных систем семейств Windows и Unix
48. Проблемы безопасности web-сайтов, как комплексных информационных систем
49. Исследование алгоритмов стеганографии в аудио-файлах
50. Анализ преимуществ и недостатков осуществления безопасных онлайн-платежей
51. Мониторинг безопасности в публичном облаке
52. Защита информации в беспроводной связи
53. Исследование методов защиты от социальной инженерии
54. Разработка безопасных приложений с применением SAST инструментов
55. Инструменты криминалистического анализа цифровых устройств
56. Защищенность операционных систем Windows различных поколений
57. Скриптовые пакеты для автоматизированного управления компьютерными сетями
58. Визуализация работы симметричных алгоритмов криптографии
59. Анализ стеганографических методов
60. Методы обнаружения местоположения злоумышленника и реагирование на инцидент
61. Мониторинг сетевой безопасности с помощью сканирования
62. Безопасность технологий удаленных рабочих столов
63. Создание безопасного мобильного приложения для страховой компании
64. Разработка мобильного приложения "Безопасный DNS"
65. Модели информационной безопасности, требования и основные этапы реализации информационной безопасности
66. Анализ сетевого трафика с помощью Wireshark
67. Расследование инцидентов кражи данных через социальные сети
68. Обнаружение утечки в информационной системе организации
69. Атаки "living off the land", опасность и проблемы противодействия
70. Анализ облачных сервисов в системах электронного документооборота

71. Исследование методов тестирования на проникновение с помощью Kali Linux
72. Методы проникновения в корпоративные ИТ-системы
73. Анализ информационной безопасности в сети 5G
74. Проведение анализа по оценке рисков организаций
75. Методы детектирования кибератак в корпоративных сетях
76. Анализ методов защиты от кибербулинга
77. Исследование алгоритмов стеганографии в видео-файлах
78. Аудит информационной безопасности в системе защиты данных предприятия
79. Исследование проблемы обеспечения информационной безопасности смарт-контрактов в блокчейне на платформе Ethereum
80. Разработка программной реализации криптографического алгоритма хеширования, основанного на модифицированной схеме "Sponge"
81. Поиск уязвимостей операционных систем
82. Исследование проблемы обеспечения информационной безопасности на платформе Hyperledger Fabric
83. Эксплуатация уязвимости информационных ресурсов
84. Способы повышения устойчивости информационных систем в условиях кибератак
85. Исследование криптографических методов языка Java
86. Методы оценки защищённости веб-сайтов
87. Современные методы и инструменты оценки угроз информационной безопасности
88. Защита web-сайтов от SQL-инъекций
89. Анализ защищенности Интернет-ресурсов по результатам пентестирования
90. Обнаружение сетевых атак с помощью технологии Honeypot
91. Оценка рисков информационной безопасности на предприятиях с разработкой мер по сохранению целостности информационных активов
92. Криминалистическая экспертиза энергозависимой памяти ОС Windows
93. Анализ и методы обхода Web-Application Firewall
94. Методы обеспечения безопасности в СУБД MySQL
95. Особенности обеспечения безопасности различных видов защищаемой информациии
96. Анализ угроз информационной безопасности для защищённой локальной вычислительной сети предприятий
97. Развитие технологий антивирусной защиты
98. Применение инструмента Wireshark для решения вопросов безопасности компьютерных сетей
99. Автоматизация реагирования на инциденты с помощью интеграции средств защиты информации
100. Методы обеспечения информационной безопасности в системах охранного видеонаблюдения
101. Методы мониторинга и обнаружения угроз информационной безопасности
102. Применение средств MS SQL Server для обеспечения защиты реляционной базы данных
103. Исследование систем генерации синтетического медиа контента
104. Организация мультикластерных SIEM-систем с реагированием на инциденты
105. Методы обеспечения информационной безопасности мобильного приложения

106. Анализ логов приложений с помощью Splunk SIEM: разработка приложения для синтетических анализов данных и инцидентов безопасности
107. Способы обнаружения и предотвращения уязвимостей Web- сайтов
108. Построение доверенной корпоративной сети предприятия на основе технологии VPN
109. Применение технологии DLP для защиты ресурсов корпоративной сети предприятия
110. Защита от утечки конфиденциальной информации в корпоративных сетях предприятия
111. Анализ видов атак типа SQL-инъекции и методов противодействия им
112. Комплексная аттестация информационных систем критически важных объектов безопасности
113. Разработка комплекса мер для анализа инцидентов
114. Методика отнесения объектов информатизации к критически важным объектам информационной-коммуникационной инфраструктуры
115. Тестирование на проникновение корпоративной структуры и ее связь с мониторингом защищённости
116. Разработка методик идентификаций (отечественного/редкого) ПО в проходящем трафике через межсетевые экраны
117. Внедрение NGFW-системы для обеспечения комплексной защиты периметра корпоративной сети
118. Методы противодействия отладке и их нейтрализация
119. Использование MITRE ATT&CK в работе аналитика SOC
120. Автоматизация реагирования на инциденты с помощью интеграции средств защиты информации
121. Внедрение NGFW-системы для обеспечения комплексной защиты периметра корпоративной сети
122. Исследование систем генерации синтетического медиа контента
123. Методика отнесения объектов информатизации к критически важным объектам информационной-коммуникационной инфраструктуры
124. Организация мультикластерных SIEM-систем с реагированием на инциденты
125. Оценка рисков информационной безопасности на предприятиях с разработкой мер по сохранению целостности информационных активов
126. Расследование инцидентов на основе методов сетевой форензики

5В100200 -«Ақпараттық қауіпсіздік жүйелері» мамандығы бойынша 2021-2022 оқу жылына арналған дипломдық жұмысының тақырыбы

1. Хакерлік утилиталар мен зиянды бағдарламаларға қарсы тұру технологиялары
2. Веб-қосымшалардың аутентификациясының осалдығы мен кемшіліктері және оны реттеу тәсілдері
3. Cloud Storage Firebase көмегімен ақпаратты қорғау
4. Жергілікті желіде хабарламаларды қауіпсіз жіберу үшін арна әзірлеу
5. Мәліметтерді клиент жақта сақтауды зерттеу
6. Криптокодтау әдісін жүзеге асыру
7. Telegram Api-ді қолдануымен екі факторлы аутентификация
8. Ашық кілтті инфраструктураны қолдау Java құралдарын зерттеу
9. SS7 желілерінің осалдықтарымен қауіпсіздік шаралары
10. Телемедицина желілеріндегі жеке деректерді қорғау және ақпараттық қауіпсіздікті қамтамасыз ету
11. Төлем жүйелерінің ақпараттық қауіпсіздігін қамтамасыз ету
12. Rest api деректерді жіберу талдауы
13. Веб-сайттардың қауіпсіздігін қамтамасыз ету әдістері
14. Бұлттық есептеулердегі көп факторлы аутентификация
15. Python тілінің көмегімен Penetration Testing әдістерін зерттеу
16. Компьютерлік вирустар мен антивирустық программалардың жұмыс жасау принциптері
17. Веб-приложениені тестілеу үшін автоматтандырылған фреймворк әзірлеу
18. Post-Initial ақырлы автоматтарының криптожүйелерді құруда қолданылуын зерттеу
19. Кибершабуылдардан қорғау әдістерін әзірлеу
20. Сниффинг технологиялары арқылы желілік трафикті анықтау
21. Ақпаратты қорғау жүйелерінің ақпараттық қауіпсіздік моделінің барабарлығын бағалау әдістері мен критерийлері
22. Java тілі үшін CERT Oracle қауіпсіз кодтау стандарттарын зерттеу
23. Программамен анықталатын желілердің осалдықтары
24. Зиянды бағдарламаларды динамикалық талдау әдістерін зерттеу
25. “Студенттер мен жұмыс берушілерге арналған цифрлық алаң" қорғалған web-қосымшасын әзірлеу
26. SEO компаниясының жергілікті желісі үшін ақпараттық қауіпсіздік жүйесін әзірлеу
27. Ssl хаттамаларының қауіпсіздік әдістерін зерттеу
28. Ақпараттық қауіпсіздік жүйелерінің сапасын бағалау әдістері мен әдістемелері
29. Компьютерлік қылмыстардан қорғау әдістері мен тәсілдері
30. Корпоративтік желілердегі мобильді абоненттік құрылғылардың қауіпсіздігін басқару әдістерін зерттеу
31. VPN технологиясын пайдалана отырып, қауіпсіз корпоративтік желісін әзірлеу
32. Қоршаған орта мен денсаулыққа мониторинг жасау үшін қолданылатын мобильді қосымшаларды зерттеу
33. IpSec және IKE негізінде виртуалды қауіпсіз желілерді зерттеу
34. Вирустық шабуылдарды жүзеге асыру жағдайында жеке деректерді қорғауды ұйымдастыру

35. Дауыс берудің криптографиялық протоколының бағдарламалық қамтамасыз етуін әзірлеу
36. Ақпараттық жүйелердің дерекқорларын масштабтау және оңтайландыру әдістерін зерттеу
37. Белгілі бір уақыт ішінде хабарламаларды шифрлаудың криптографиялық протоколының бағдарламалық қамтамасыз етуін әзірлеу
38. Графикалық файлдардағы стеганография алгоритмдерін зерттеу
39. ARP-spoofing типті шабуылдарды анықтау мен алдын-алудың таратылған жүйелерін зерттеу
40. Зиянды бағдарламаларды статикалық талдау әдістерін зерттеу
41. Қолжетімділікті бақылау және басқару жүйесі
42. Компаниялардағы антивирустық қауіпсіздік кешендерін жасау әдістерін зерттеу
43. Инциденттерді желілік форензика әдістері негізінде зерттеу
44. Веб-скрапингтен қорғану әдістері
45. Биометрикалық аутентификация әдістерінің мобильді құрылғыларындағы қолданысын зерттеу
46. Threat Intelligence Platform класының шешімдері негізінде ақпараттық қауіпсіздік инциденттеріне әрекет ету процесін автоматтандыру
47. Windows және Unix операциялық жүйелерін криминалистикалық сараптау әдістері
48. Веб-сайттардың қауіпсіздік мәселелері күрделі ақпараттық жүйе ретінде
49. Аудио файлдардағы стеганография алгоритмдерін зерттеу
50. Қауіпсіз онлайн-төлемдерді жүзеге асырудың артықшылықтары мен кемшіліктерін талдау
51. Қоғамдық бұлттағы қауіпсіздікті бақылау
52. Сымсыз байланыстағы ақпаратты қорғау
53. Әлеуметтік инженериядан қорғау әдістерін зерттеу
54. SAST құралдарын қолданып, қауіпсіз қосымшаларды әзірлеу
55. Цифрлық құрылғыларды криминалистикалық талдау құралдары
56. Әр түрлі буындағы Windows операциялық жүйелерінің қауіпсіздігі
57. Компьютерлік желілерді автоматты түрде басқаруға арналған скриптік пакеттер
58. Симметриялық криптография алгоритмдерінің жұмысын визуализациялау
59. Стеганографиялық әдістерге талдау жасау
60. Шабуылдаушының орнын анықтау әдістері және шабуылға жауап беру
61. Сканерлеу арқылы желі қауіпсіздігі мониторингін жүргізу
62. Қашықтағы жұмыс үстелі технологиясының қауіпсіздігі
63. Сақтандыру компаниясы үшін қауіпсіз мобильді қосымшаны құру
64. «Қауіпсіз DNS» мобильді қосымшасын әзірлеу
65. Ақпараттық қауіпсіздік модельдері, ақпараттық қауіпсіздікті іске асырудың талаптары мен негізгі кезеңдері
66. Wireshark бағдарламасының көмегімен желілік трафикті талдау
67. Әлеуметтік желілер арқылы деректерді ұрлау оқиғаларын тергеу
68. Ұйымның ақпараттық жүйесіндегі ақпараттың жайылуын анықтау
69. "Living off the land" шабуылы, қаупі және қарсы шаралар мәселелері
70. Электрондық құжат айналымы жүйелерінде бұлтты қызметтерді талдау
71. Kali Linux көмегімен Penetration Testing әдістерін зерттеу

72. Корпоративтік АТ-жүйелеріне ену әдістері
73. 5G желісіндегі ақпараттық қауіпсіздікті талдау
74. Ұйымдардың тәуекелдерін бағалау бойынша талдау жүргізу
75. Корпоративтік желілердегі кибершабуылдарды анықтау әдістері
76. Кибербулингтен қорғану тәсілдерін талдау
77. Бейне файлдардың стеганография алгоритмдерін зерттеу
78. Кәсіпорынның деректерін қорғау жүйесіндегі ақпараттық қауіпсіздік аудиті
79. Ethereum платформасындағы блокчейндегі ақылды келісімшарттардың ақпараттық қауіпсіздігін қамтамасыз ету мәселесін зерттеу
80. Өзгертілген "Sponge" схемасы негізінде криптографиялық хэширлеу алгоритмін бағдарламалық қамтамасыз етуді әзірлеу
81. Операциялық жүйенің осал тұстарын іздеу
82. Hyperledger Fabric платформасында ақпараттық қауіпсіздікті қамтамасыз ету мәселесін зерттеу
83. Search for operating system vulnerabilities
84. Кибершабуылдар жағдайында ақпараттық жүйелердің тұрақтылығын арттыру жолдары
85. Java тілінің криптографиялық әдістерін зерттеу
86. Веб-сайттардың қорғалуын бағалау әдістері
87. Ақпараттық қауіпсіздік қауіп қатерлерін бағалаудың заманауи әдістері мен құралдары
88. Web-сайттарды SQL инъекциясынан қорғау
89. Пентестирлеу нәтижелері бойынша Интернет-ресурстардың қорғалуын талдау
90. Honeypot технологиясы қамтамасы көмегімен желілік шабуылдарды анықтау
91. Кәсіпорындардағы ақпараттық активтердің тұтастығын сақтау бойынша шараларды әзірлеумен ақпараттық қауіпсіздік тәуекелдерін бағалау
92. Windows операциялық жүйесінің энерготәуелді жадысының криминалистикалық сараптамасы
93. Веб-қосымшалардың брандмауэрін талдау және айналып өту әдістері
94. MySQL ДҚБЖ ортасында қауіпсіздікті қамтамасыз ету әдістері
95. Қорғалатын ақпараттың әртүрлі түрлерінің қауіпсіздігін қамтамасыз ету ерекшеліктері
96. Кәсіпорындардың қорғалатын жергілікті желісіне ақпараттық қауіпсіздік қатерлерін талдау
97. Вирусқа қарсы қорғау технологияларын дамыту
98. Wireshark құралын компьютерлік желілер қауіпсіздігі мәселелерін шешуде қолдану
99. Ақпараттық қауіпсіздік құралдарын біріктіру арқылы оқыс оқиғаларға әрекет етуді автоматтандыру
100. Бейнебақылау жүйелеріндегі ақпаратты қорғау әдістері
101. Ақпараттық қауіпсіздік қатерлерін мониторингілеу және анықтау әдістері
102. Реляциялық деректер базасын қорғауды қамтамасыз ету үшін MS SQL Server құралдарын қолдану
103. Синтетикалық медиа контент генерациялау жүйелерін зерттеу
104. Инцидентерге жауап беретін көп кластерлі SIEM-жүйелерін ұйымдастыру
105. Мобильді қосымшаның ақпараттық қауіпсіздігін қамтамасыз ету әдістері

106. Splunk SIEM көмегімен қолданбалар журналдарын талдау: деректерді синтетикалық талдау мен қауіпсіздік инциденттерге арналған қосымшаны әзірлеу
107. Web - сайттардың осалдықтарын анықтау және алдын алу әдістері
108. VPN технологиясы негізінде кәсіпорынның сенімді корпоративтік желісін құру
109. Кәсіпорынның корпоративтік желісінің ресурстарын қорғау үшін DLP технологиясын қолдану
110. Кәсіпорынның корпоративтік желілерінде құпия ақпараттың сыртқа кетуінен қорғау
111. SQL-инъекция сияқты шабуыл түрлеріне және оларға қарсы тұру әдістеріне талдау жүргізу
112. Қауіпсіздіктің аса маңызды объектілерінің ақпараттық жүйелерін кешенді аттестаттау
113. Инциденттерді талдау бойынша шаралар кешенін әзірлеу
114. Ақпараттандыру объектілерін ақпараттық-коммуникациялық инфрақұрылымның маңызды объектілеріне жатқызу әдістемесі
115. Корпоративтік құрылымның еңгізу сынағы және оның қауіпсіздік мониторингімен байланысы
116. Желіаралық экран арқылы трафикті өткізу кезінде бағдарламалық қамтамасыз етуді идентификациялау әдістерін (отандық/ сирек) әзірлеу
117. Корпоративтік желінің периметрін кешенді қорғауды қамтамасыз ету үшін NGFW-жүйесін енгізу
118. Отладкаға қарсы әрекет және бейтараптандыру әдістері
119. SOC талдаушысының жұмысында MITRE ATT&CK пайдалану
120. Ақпараттық қауіпсіздік құралдарын біріктіру арқылы оқыс оқиғаларға әрекет етуді автоматтандыру
121. Корпоративтік желінің периметрін кешенді қорғауды қамтамасыз ету үшін NGFW-жүйесін енгізу
122. Синтетикалық медиа контент генерациялау жүйелерін зерттеу
123. Ақпараттандыру объектілерін ақпараттық-коммуникациялық инфрақұрылымның маңызды объектілеріне жатқызу әдістемесі
124. Инциденттерге жауап беретін көп кластерлі SIEM-жүйелерін ұйымдастыру
125. Кәсіпорындардағы ақпараттық активтердің тұтастығын сақтау бойынша шараларды әзірлеумен ақпараттық қауіпсіздік тәуекелдерін бағалау
126. Инциденттерді желілік форензика әдістері негізінде зерттеу

Topics of theses
on speciality 5B100200 – Information Security Systems
2021-2022 academi years

1. Technologies for countering hacker utilities and malware
2. Studying of authentication security vulnerabilities in web applications and identifying methods to resolve them.
3. Information protection by using Cloud Storage Firebase
4. Implementation of a channel for secure messages transfer in a local area network
5. Exploring client-side data saving
6. Implementation of the cryptocoding method
7. Two-factor authentication using Telegram Api
8. Exploring Java Tools to Support Public Key Infrastructure
9. Vulnerabilities and Security Methods of SS7 Networks
10. Personal data protection and information security in telemedicine networks
11. Ensuring information security of payment systems
12. Rest api data transfer analysis
13. Methods for providing website security
14. Multi-factor authentication in cloud computing
15. Investigating Penetration Testing Methods Using Pytho
16. Computer viruses and the principles of antivirus programs
17. Development of a framework for automated testing of web applications
18. Research of application of finite machines Post- Initial for construction of cryptosystems
19. Development of methods of protection against cyber attacks
20. Network traffic sniffing technologies
21. Methods and criteria for assessing the adequacy of the information security model of information security systems
22. Exploring Oracle CERT Secure Coding Standards for Java
23. Software-defined network vulnerabilities
24. Research of methods for dynamic analysis of malware
25. Development of a secure web-application "Digital platform for students and employers"
26. Development of an information security system for a local area network of an SEO company
27. Research of ssl protocol security methods
28. Methods and techniques for assessing the quality of information security systems
29. Methods and ways of protection against computer crimes
30. Research of methods of security management of mobile subscriber devices in corporate networks
31. Development of a secure corporate network using VPN technology
32. The study of mobile applications used for environmental and health monitoring
33. Investigation of virtual secure networks based on IpSec and IKE
34. Organization of personal data protection in the context of the implementation of virus attacks
35. Development of a software implementation of a cryptographic voting protocol
36. Research of methods of scaling and optimization of information systems databases

37. Development of a software implementation of a cryptographic protocol for encrypting messages for a preassigned time
38. Search for operating system vulnerabilities
39. Studies on image steganography algorithms
40. Research of a distributed system for detecting and preventing ARP-spoofing attacks
41. Research of methods of static analysis of malware
42. Access control and management system
43. Research of methods of development of anti-virus security complexes in the company
44. Incidents investigation based on network forensics methods
45. Protection Methods against Web Scraping
46. Study of the use of biometric authentication methods in mobile devices
47. Automation of the information security incident response process based on Threat Intelligence Platform class solutions
48. Methods of Forensic Examination of Windows and Unix Operating Systems
49. Security problems of websites as complex information systems
50. Studies on audio steganography algorithms
51. Analysis of advantages and disadvantages of making secure online payments
52. Security monitoring in public cloud
53. Protection of information in wireless communication
54. Studies on the Social Engineering Defense methods
55. Development of secure applications by using SAST tools
56. Forensic analysis tools for digital devices
57. Security of Windows Operating Systems of Different Generations
58. Script Packages for Automated Computer Networks Management
59. Visualization of the Work of Symmetric Cryptography Algorithms
60. Analysis of steganographic methods
61. Methods for determining the location of the attacker and responding to incidents
62. Monitoring of network security with scanning
63. Remote Desktop Technologies Security
64. Creating a secure mobile application for an insurance company
65. Development of a mobile application "Safe DNS"
66. Information security models, requirements and main stages of information security implementation
67. Analysis of network traffic using Wireshark
68. Investigation of data theft incidents through social networks
69. Leak detection in an organization’s information system
70. "Living off the land" attacks, danger and problems of countermeasures
71. Analysis of cloud services in electronic document management systems
72. Investigating Penetration Testing Methods with Kali Linux
73. Methods of penetration into corporate IT systems
74. Analysis of information security in the 5G network
75. Carrying out an analysis to assess the risks of organizations
76. Methods of detecting cyber attacks in corporate networks
77. Analysis of ways to protect against cyberbullying
78. Studies on video steganography algorithms

79. Audit of information security in the enterprise data protection system
80. Research of the problem of providing the information security of smart contracts in the blockchain on the Ethereum platform
81. Researching the problem of providing information security on the Hyperledger Fabric platform
82. Exploitation of the vulnerability of information resources
83. Methods for increasing the resilience of information systems in the context of cyber attacks
84. Investigating Cryptographic Methods of the Java Language
85. Methods for evaluating website security
86. Analysis of methods of protection against cyberbullying
87. Protecting Web-sites from SQLl Injection
88. Analysis of the security of Internet resources based on the results of penetration testing
89. Detecting network attacks using Honeypot technology
90. Assessment of information security risks at the enterprises and development of measures to preserve the integrity of information assets
91. Forensic analysis of the energy-dependent memory of the Windows operating system
92. Web Application Firewall Analysis and Bypass Techniques
93. Methods for providing security in MySQL DBMS
94. Features of ensuring the security of various types of protected information
95. Analysis of information security threats to a protected local area network of enterprises
96. Development of anti-virus protection technologies
97. Using the Wireshark tool to solve computer network security issues
98. Automatization of an incident response with the information security tools integration
99. Methods of information security in video surveillance systems
100. Methods of monitoring and detection of information security threats
101. Using the MS SQL Server tools to ensure the protection of a relational database
102. Research of the synthetic media content generation systems
103. Organization of multi-cluster SIEM systems with incident response
104. Methods of ensuring the information security of a mobile application
105. Application Log Analysis using the Splunk SIEM: Application development for synthetic data analysis and security incidents
106. Methods for detecting and preventing Web - site vulnerabilities
107. Building a trusted corporate enterprise network based on VPN technology
108. The use of DLP technology to protect the resources of the corporate network of the enterprise
109. Protection against leakage of confidential information in corporate networks of the company
110. Analysis of types of attacks such as SQL injection and methods of countering them
111. Comprehensive certification of information systems of critical security facilities
112. Development of a set of measures for analyzing incidents
113. Methodology for informatization objects classifying as critically important objects of information and communication infrastructure
114. Penetration testing of the corporate structure and its relationship with security monitoring
115. Methodology development of software identification (domestic/rare) in ongoing traffic via firewalls

116. NGFW system implementation for providing comprehensive protection of the corporate network perimeter
117. Debugging counteraction and neutralization methods
118. Development of a software implementation of a cryptographic hashing algorithm based on a modified "Sponge" scheme
119. Using MITRE ATT&CK in the work of a SOC analyst
120. Automatization of an incident response with the information security tools integration
121. NGFW system implementation for providing comprehensive protection of the corporate network perimeter
122. Research of the synthetic media content generation systems
123. Methodology for informatization objects classifying as critically important objects of information and communication infrastructure
124. Organization of multi-cluster SIEM systems with incident response
125. Assessment of information security risks at the enterprises and development of measures to preserve the integrity of information assets
126. Incidents investigation based on network forensics methods