«Әл-Фараби атындағы ҚазҰУ»
КЕАҚ Ғылыми кеңес отырысында
16.06.2026 ж. № 14 хаттамамен
БЕКІТІЛДІ

D095 – «Ақпараттық қауіпсіздік» білім беру бағдарламалары тобына докторантураға түсушілерге арналған емтихан бағдарламасы

1. Жалпы ережелер

1. Бағдарлама «Жоғары және жоғары оқу орнынан кейінгі білімнің білім беру бағдарламаларын іске асыратын білім беру ұйымдарына оқуға қабылдаудың үлгілік қағидаларын бекіту туралы» Қазақстан Республикасы Білім және ғылым министрінің 2018 жылғы 31 қазандағы № 600 бұйрығына (бұдан әрі – үлгілік қағидалар) сәйкес жасалды.

2. Докторантураға түсу емтиханы сұхбаттасудан, эссе жазудан және білім беру бағдарламалары тобының бейіні бойынша емтиханнан тұрады.

Блогы	Балы
1. Сұхбаттасу	30
2. Эссе	20
3. Білім беру бағдарламасы тобының бейіні бойынша емтихан	50
Барлығы/ өту ұпайы	100/75

3. Түсу емтиханының ұзақтығы – 3 сағат 10 минут, осы уақыт ішінде оқуға түсуші эссе жазады, электрондық емтихан билетіне жауап береді. Сұхбаттасу ЖОО қабылдау емтиханының алдында өткізіледі.

2. Түсу емтиханын өткізу тәртібі.

1. D095 - «Ақпараттық қауіпсіздік» білім беру бағдарламалары тобына докторантураға түсушілер проблемалық / тақырыптық эссе жазады. Эссе көлемі – 250-300 сөзден кем болмауы керек.

2. Электрондық емтихан билеті 3 сұрақтан тұрады.

Білім беру бағдарламасы тобының бейіні бойынша емтиханға дайындалуға арналған тақырыптар.

«Ақпараттық қауіпсіздік жүйелерін ұйымдастыру» пәні

Тақырыбы: Ақпараттық қауіпсіздікті қамтамасыз етудің заманауи тұжырымдамалары мен технологиялары

Тақырыпшалар:

1. Ақпараттық қауіпсіздікті қамтамасыз етудің заманауи тәсілдері. Zero Trust Architecture (Нөлдік сенім архитектурасы) тұжырымдамасы. Цифрлық трансформация жағдайындағы корпоративтік қауіпсіздік архитектурасы. Zero Trust Architecture жүйесіндегі сенімді формализациялау мәселесі. Контекст параметрлері (пайдаланушы, құрылғы, мінез-құлық, орналасқан жері, сессия тәуекелі, қорғалатын ресурстың сезімталдық деңгейі).

2. ISO/IEC 27001, NIST Cybersecurity Framework 2.0 және тәуекелге бағдарланған басқару қағидаттары негізінде ақпараттық қауіпсіздік процестерінің жетілу моделін құрудың зерттеу тәсілі.

3. Security Operations Center (SOC) архитектурасы және жұмыс істеу қағидаттары. Оқиғаларды анықтау және оларға әрекет ету үшін қолданылатын SIEM, SOAR және XDR класты жүйелер. SIEM, SOAR және XDR технологияларын пайдалану арқылы инциденттерге әрекет етуді автоматтандыру кезіндегі ғылыми мәселелер. Оқиғаларды корреляциялау сапасын, инциденттерді басымдыққа бөлу және автоматты шешімдердің тиімділігін бағалау.

4. Кибертәуекелдерді басқару. Тәуекелдерді сәйкестендіру, талдау және бағалау әдістемелері. Тәуекелдерді бағалаудың сандық және сапалық әдістері. Қауіп-қатер модельдерін құру. Қолданбалы тәуекел бағалауы мен ғылыми кибертәуекел моделінің айырмашылықтары. Активтерді, қауіптерді, осалдықтарды, ықтималдықты, залалды, белгісіздікті және қалдық тәуекелді ескеретін модель. Lateral movement, есептік жазбалардың компрометациясы, артық артықшылықтар және рұқсатсыз қолжетімділік тәуекелдерінің төмендеуін бағалау метрикалары.

5. Кибербарлау (Cyber Threat Intelligence). Киберқауіптер туралы деректер көздері. Қауіптердің таксономиясы. Cyber Kill Chain моделі. MITRE ATT&CK матрицасы және оны шабуылдарды талдауда пайдалану. Қарсылас әрекеттерін сипаттайтын модельдер ретінде MITRE ATT&CK пен Cyber Kill Chain салыстыруы.

6. Компьютерлік шабуылдарды анықтау әдістері. Қауіптерді анықтаудың сигнатуралық, эвристикалық және интеллектуалды әдістері. IDS, IPS, NDR және EDR жүйелері. False Positive, False Negative, class imbalance, latency және қате құны факторларын ескере отырып шабуылдарды анықтау сапасын бағалау әдістемесі.

7. Ақпараттық қауіпсіздік міндеттеріндегі машиналық оқыту әдістері. Желілік трафиктегі аномалияларды анықтау. Жасанды интеллект әдістерін пайдалана отырып шабуылдарды жіктеу. Желілік шабуылдарды анықтауға арналған машиналық оқыту модельдерінің жалпылау қабілетін зерттеу мәселесі. Dataset Shift, Concept Drift, сыныптардың теңгерімсіздігі және ескірген деректер жиынтықтарының нәтижелердің сенімділігіне әсері.

8. Киберқауіпсіздік жүйелеріндегі терең оқыту. Конволюциялық нейрондық желілерді (CNN), рекурренттік нейрондық желілерді (RNN), ұзақ қысқа мерзімді жады желілерін (LSTM), басқарылатын рекурренттік блоктарды (GRU) және Transformer-модельдерін басып кірулерді анықтау және зиянды бағдарламаларды талдау міндеттерінде қолдану барысында туындайтын ғылыми мәселелер.

9. Қазақстан Республикасының нормативтік-құқықтық құжаттары. Қазақстан Республикасының «Ақпаратқа қол жеткізу туралы» Заңына шолу. Қазақстан Республикасының мемлекеттік құпияларына қол жеткізілген немесе бұрын қол жеткізген азаматтардың құқықтарын шектеу мәселелері. Дербес деректерді қорғау саласындағы Қазақстан Республикасы Қылмыстық

кодексінің баптары. Қазақстан Республикасы Үкіметінің дербес деректерді қорғау саласындағы құзыреттері.

10. Аудио-визуалды дипфейктерді анықтау әдістері. Генеративті модельдердің архитектуралары. Синтетикалық контентті анықтау әдістері. Мультимедиялық деректердің шынайылығын бағалау. Аудио-визуалды deepfake анықтау – цифрлық деректерге деген сенімнің техникалық және әдіснамалық мәселесі. Deepfake detector жүйелерінің жаңа генеративті модельдерге, қысуға, шудың әсеріне және белгісіз деректер жиынтықтарына төзімділігін бағалау хаттамасы.

11. Бұлттық қауіпсіздік. IaaS, PaaS және SaaS модельдері. Shared Responsibility Model тұжырымдамасы. Бұлттық инфрақұрылым қауіпсіздігін басқару. IaaS, PaaS және SaaS орталарында cloud provider мен cloud tenant арасындағы кибертәуекелдерді бөлу моделі. Multi-cloud және hybrid-cloud орталарындағы Shared Responsibility Model шектеулері.

12. Контейнерлендірілген және микросервистік қосымшалардың қауіпсіздігі. Docker және Kubernetes технологиялары. Cloud-native қосымшаларын қорғау. Ашық дереккөздерден алынған деректерді талдау және жабық дереккөздерге қол жеткізу кезіндегі белсенді шабуыл векторлары. Контейнерлендірілген қосымшалардағы бағдарламалық қамтамасыз ету жеткізу тізбегінің тәуекелдерін ғылыми бағалау. Образдардың, registry жүйелерінің, CI/CD pipeline процестерінің, тәуелділіктердің, SBOM, артефактілерге қол қою және рұқсат беру саясаттарының осалдықтары.

13. Заттар интернеті (IoT) және өнеркәсіптік жүйелердің (IIoT) қауіпсіздігі. Таратылған құрылғылардың осалдықтары. Киберфизикалық жүйелерді қорғау әдістері. Цифрлық трансформация, қашықтан жұмыс, SaaS сервистері, бұлттық технологиялар, мобильді құрылғылар және IoT жағдайында ақпараттық қауіпсіздік архитектурасын құрудың жаңа ғылыми мәселелері.

14. Кибершабуылдарды атрибуциялау. Шабуыл көздерін сәйкестендіру әдістері. Threat Intelligence, OSINT және мінез-құлықтық талдау арқылы атрибуция жүргізу. Кибершабуылдарды атрибуциялаудағы эпистемологиялық және әдіснамалық шектеулер. Деректердің толық еместігі, False Flag операциялары, TTP үлгілерін көшіру, жария құралдар, OSINT және сенімділік деңгейлері.

15. Ақпараттық қауіпсіздіктің дамуындағы перспективалы бағыттар. Автономды қорғаныс жүйелері. Кибертұрақтылық. Инциденттерге әрекет ету жөніндегі шешімдерді қабылдау жүйелеріндегі жасанды интеллект. Инциденттерге автоматтандырылған әрекет етуде жасанды интеллектті қолданудың ғылыми мәселелері.

«Ақпаратты қорғау құралдарының элементтері» пәні

Тақырыбы: Компьютерлік жүйелердегі ақпаратты қорғау

Тақырыпшалар:

1. Заманауи компьютерлік жүйелердің архитектурасы. Есептеу жүйелерінің модельдері (жергілікті, таратылған, бұлттық). Компьютерлік

жүйелердегі деректер ағындары. Жүйе архитектурасындағы ақпараттық қауіпсіздікті қамтамасыз етудің негізгі қағидаттары.

2. Компьютерлік жүйелердегі қауіп-қатер моделі. Қауіптердің жіктелуі: ішкі және сыртқы, қасақана және кездейсоқ. Ақпараттың сыртқа шығу арналары. Бұзушы моделі және оның мүмкіндіктері. Ақпараттық қауіпсіздік тәуекелдерін бағалау.

3. Заманауи операциялық жүйелердегі қолжетімділікті бақылау механизмдері. Дискрециялық және мандаттық қолжетімділік модельдері. Рөлдік қолжетімділікті басқару (RBAC). Атрибуттық модельдер (ABAC).

4. Пайдаланушыларды сәйкестендіру және аутентификациялаудың заманауи әдістері. Биометриялық технологиялар, көп факторлы аутентификация, аппараттық токендер. Таратылған жүйелердегі аутентификация хаттамалары.

5. Қауіпсіздік журналдары мен мониторинг жүйелері. Қауіпсіздік оқиғаларын журналдау, қолжетімділік журналдарын талдау. SIEM жүйелері және оқиғаларды корреляциялау. Аномальды белсенділікті анықтау.

6. Компьютерлік жүйелердегі деректер тұтастығы. Файлдар мен процестердің тұтастығын бақылау әдістері. Бақылау қосындылары, хэштеу, электрондық цифрлық қолтаңба. Нақты уақыт режимінде деректерді өзгертуге қарсы қорғаныс.

7. Ақпаратты қорғаудың бағдарламалық-аппараттық құралдары. TPM сенімді платформалық модульдерінің архитектурасы. HSM аппараттық қауіпсіздік модульдері. Криптографиялық функцияларды аппараттық қамтамасыз етуге енгізу.

8. Компьютерлік жүйелердің аппараттық құрамдастарын қорғау. Қорғалатын ресурстардың жіктелуі: процессор, жад, перифериялық құрылғылар. Физикалық қолжетімділік пен аппараттық шабуылдардан қорғау әдістері.

9. Бағдарламалық қамтамасыз етуді заңсыз көшіруден қорғау. Бағдарламалық қамтамасыз етуді лицензиялау. Аппараттық қорғаныс кілттері. Бағдарламаларды аппараттық платформаға және цифрлық идентификаторларға байланыстыру.

10. Компьютерлік жүйелердегі құпия ақпаратты басқару. Құпиясөздер мен криптографиялық кілттерді сақтау. Қауіпсіз сақтау жүйелері (Key Vault, Secure Enclave). Құпияларды басқару саясаттары.

11. Криптографиялық кілттердің өмірлік циклі. Кілттерді генерациялау, тарату, сақтау, жаңарту және жою. Кілттерді басқарудың орталықтандырылған және орталықтандырылмаған модельдері (KMS).

12. Симметриялық аутентификация және кілттерді тарату хаттамалары. Kerberos жүйесі орталықтандырылған аутентификация жүйесінің мысалы ретінде. Кілттерді тарату орталығының сенімді механизмдері.

13. Асимметриялық аутентификация хаттамалары. Ашық кілттер инфрақұрылымын (PKI) пайдалану. Сертификаттарды тексеру, сенім тізбегі, сертификаттарды қайтарып алу (CRL, OCSP).

14. Кілттік ақпаратты сақтау мен қорғауды ұйымдастыру. Аппараттық және бағдарламалық кілт тасымалдағыштары. Смарт-карталар, токендер, TPM модульдері. Кілттерді көшіруден және алудан қорғау әдістері.

15. Бағдарламалық қамтамасыз етуді кері жобалау және талдаудан қорғау. Бағдарламаларды статикалық және динамикалық талдау әдістері. Код обфускациясы, антиотладкалық механизмдер, дизассемблирлеу мен реверс-инжинирингтен қорғау.

«Компьютерлік ақпаратты қорғау әдістері мен құралдары» пәні

Тақырыбы: Криптоталдау

Тақырыпшалар:

1. Классикалық шифрлар және оларды бұзу әдістері. Цезарь және аффиндік шифрларды дешифрлау және толық іздеу әдісімен бұзу. Орынбасу шифрларын жиілік әдісімен талдау. Қазақ және орыс тілдеріндегі мәтіндер үшін классикалық шифрлардың кемшіліктері мен жиіліктік талдауы.

2. Бүтін сандар сақинасы, Евклид алгоритмі және оның салдарлары. Ең үлкен ортақ бөлгішті көрсету. Салыстырулар теориясы. Берілген модуль бойынша салыстырулардың қасиеттері. Қайтымды элементтер.

3. Эйлер функциясы және оның қасиеттері. Жай сандар үшін Эйлер функциясы. Эйлер функциясының мультипликативтілік теоремасы. Эйлер функциясының мәндерін есептеу формуласы. Эйлер функциясын пайдаланып дәрежеге шығару.

4. Ферма–Эйлер теоремасы және RSA шифрының негізгі теоремасы.

5. RSA шифры, шифрлау және дешифрлау процесі, математикалық негіздемесі. Берілген мәтінді ашық кілтпен шифрлау. Жабық кілтпен дешифрлау.

6. RSA электрондық қолтаңбасы: идеясы және математикалық негіздемесі.

7. RSA электрондық қолтаңбасын жүзеге асыру. Құжатқа электрондық қолтаңба қою кезеңі.

8. RSA электрондық қолтаңбасын жүзеге асыру. Қолтаңбаны ашық кілт арқылы тексеру кезеңі.

9. Натурал сандар қатарындағы жай сандардың таралуы және RSA шифрының криптотұрақтылығын бағалау.

10. $<F_2; +, *>$ өрісіндегі көпмүшеліктер сақинасы. Евклид алгоритмі және екі көпмүшенің ең үлкен ортақ бөлгішін табу. Келтірілмейтін көпмүшелер. 2, 3, 4 және 5 дәрежелі келтірілмейтін көпмүшелер.

11. $<F_{2^n}; +, *>$ өрісін келтірілмейтін көпмүше бойынша қалдықтар класы ретінде құру. Қосу және көбейту амалдарын анықтау. Нөлден өзге элементтердің қосу және көбейту бойынша кері элементтері. $<F_{16}; +, *>$ өрісін құру.

12. Лагранж теоремасы: топ ретінің ішкі топ ретіне бөлінгіштігі. Элемент ретінің топ ретіне бөлінгіштігі туралы салдарлар. Zn тобының ішкі

топтарына мысалдар. $<F_{2^n}; +, *>$ өрісіндегі алғашқы элемент туралы теорема. $<F_{16}; +, *>$ өрісінің алғашқы элементтері.

13. n-разрядты екілік блоктар негізінде құрылған өріс. Қосу және көбейту амалдары. Нөлден өзге элементтердің кері элементтері. Алғашқы элементтер. 4-разрядты екілік блоктар өрісін құру және оның алғашқы элементтерін анықтау.

14. Диффи–Хеллман есебі. Қашықтағы пайдаланушылар үшін ортақ құпияны қалыптастыру. Диффи–Хеллман есебінің шешілмеу күрделілігіне негізделген кілт алмасу. Қашықтағы пайдаланушылар арасындағы кілттермен алмасу мәселесін шешу.

15. Эль-Гамаль шифры. Кілттермен алмасу процесі. Шифрлау және дешифрлау алгоритмдері. Практикалық мысал негізінде жүзеге асыру.

3. Пайдаланылған әдебиеттер тізімі.

1. Stallings W. *Cryptography and Network Security: Principles and Practice*. — 8th ed. — Pearson, 2020. — 768 p.
2. Katz J., Lindell Y. *Introduction to Modern Cryptography*. — 2nd ed. — CRC Press, 2014. — 538 p.
3. Menezes A., van Oorschot P., Vanstone S. *Handbook of Applied Cryptography*. — CRC Press, 1996. — 816 p.
4. Schneier B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. — 2nd ed. — Wiley, 1996. — 784 p.
5. Ferguson N., Schneier B., Kohno T. *Cryptography Engineering*. — Wiley, 2010. — 384 p.
6. Paar C., Pelzl J. *Understanding Cryptography*. — Springer, 2010. — 372 p.
7. Koblitz N. *A Course in Number Theory and Cryptography*. — Springer, 1994. — 236 p.
8. Diffie W., Hellman M. New Directions in Cryptography // *IEEE Transactions on Information Theory*. — 1976. — Vol. 22(6). — P. 644–654.
9. Rivest R., Shamir A., Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems // *Communications of the ACM*. — 1978. — Vol. 21(2). — P. 120–126.
10. ElGamal T. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms // *IEEE Transactions on Information Theory*. — 1985. — Vol. 31(4). — P. 469–472.
11. Shannon C. E. Communication Theory of Secrecy Systems // *Bell System Technical Journal*. — 1949. — Vol. 28. — P. 656–715.
12. Bishop M. *Computer Security: Art and Science*. — Addison-Wesley, 2003. — 1134 p.
13. Pfleeger C., Pfleeger S. L. *Security in Computing*. — 5th ed. — Pearson, 2015. — 624 p.

14. Anderson R. *Security Engineering*. — 3rd ed. — Wiley, 2020. — 1250 p.
15. Easttom C. *Modern Cryptography: Applied Mathematics for Encryption and Information Security*. — McGraw-Hill, 2021. — 600 p.
16. ISO/IEC 27001:2022. *Information Security Management Systems — Requirements*. — International Organization for Standardization, 2022.
17. ISO/IEC 27002:2022. *Information security, cybersecurity and privacy protection — Information security controls*. — ISO, 2022.
18. Фомичев В. М. *Дискретная математика и криптография*. — М.: Диалог-МИФИ, 2012. — 400 с.
19. Ященко В. В. *Введение в криптографию*. — М.: МЦНМО, 2000. — 272 с.
20. Ожигов Ю. И. *Основы защиты информации в компьютерных системах*. — М.: Горячая линия-Телеком, 2018. — 320 с.