ӘЛ-ФАРАБИ АТЫНДАҒЫ ҚАЗАҚ ҰЛТТЫҚ УНИВЕРСИТЕТІ

АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР ФАКУЛЬТЕТІ

БЕКІТІЛГЕН
әл-Фараби атындағы Қазақ ұлттық
университетінің ғылыми кеңесінің
мәжілісінде «____»_____2020 ж.
№_____ хаттамасынан

«8D06301 – АҚПАРАТТЫҚ ҚАУІПСІЗДІК ЖҮЙЕЛЕРІ» МАМАНДЫҒЫ БОЙЫНША ДОКТАРАНТУРАҒА ТҮСУШІЛЕРГЕ АРНАЛҒАН МАМАНДЫҚ БОЙЫНША ТҮСУ ЕМТИХАНЫНЫҢ БАҒДАРЛАМАСЫ

АЛМАТЫ 2020

Бағдарлама «8D06301 – Ақпараттық қауіпсіздік жүйелері» мамандығы бойынша Мемлекеттік жалпы білім беру стандартына сәйкес жасалған. Бағдарламаны құрастырушы доцент м.а. Мусиралиева Ш.Ж.

Бағдарлама Ақпараттық жүйелер кафедрасының мәжілісінде қарастырылған.
2020 ж. _____ № ___ Хаттама
Кафедра меңгерушісі _____ Мусиралиева Ш.Ж

Ақпараттық технологиялар факультеттің әдістемелік бюросында мақұлданған
2020 ж. _____ № ___ Хаттама
Әдістемелік бюро төрайымы _____ Гусманова Ф.Р.

Ғылыми кеңес мәжілісінде бекітілген
2020 ж. _____ № ___ Хаттама
Ғылыми кеңес төрағасы,
Факультет деканы _____ Урмашев Б.А.

Ғылыми хатшы _____ Самбетбаева А.К.

БАҒДАРЛАМА МАЗМҰНЫ

1. Мамандық бойынша түсу емтиханның мақсаты мен міндеттері

1.1. Мамандық бойынша оқуға түсу емтиханының мақсаты

Түсушілерге арналған емтиханның мақсаты теориялық дайындық деңгейін қарастыру, докторантураға түсушілерге конкурстық қатысу негізінде дербес ұсынылуын нақтылау.

Түсушілерге емтихан бағдарламасына келесі пәндер кіреді: «Ақпараттық қауіпсіздік жүйелерін ұйымдастыру», «Компьютерлік ақпаратты қорғаудың әдістері мен құралдары», «Ақпараттық қауіпсіздік құралдарының элементтері»

1.2. Мамандық бойынша оқуға түсу емтиханының міндеттері

Емтихан кезінде:

• Информатиканың және ақпараттық технологияның іргелі негізін; қазіргі ақпараттық технологиялардың негізгі жетістіктері мен даму тенденцияларын; кәсіби және ғылыми қызметтер технологияларын; кәсіби және ғылыми әдептің негізгі ережелерін білу және оларды өз жұмыстарында қолдана білу керек.

• Ғылыми-техникалық, табиғи-ғылыми, жалпы-ғылыми ақпаратты есеп формасына әкеліп таба, талдай және өңдей алу қажет; жаңа ғылыми нәтижелерін халық алдында көрсете алу, өзінің кәсіби, ғылыми және ғылыми-педагогикалық нәтижелерін жобалай және жүзеге асыра білу; кейінгі кәсіби өсуін жобалай білуі қажет.

• Өзіндік ғылыми-зерттеу жұмыстары мен ғылыми ізденістер дағдыларын меңгеруі; ғылыми жобада, қарапайым ғылыми және кәсіби есептерді шешу, жазбаша және ауызша формада өз ойын логикалық және дұрыс жеткізу керек.

2. PhD докторантураға тапсырушыларға арналған дайындық деңгейінің талаптары

Келесі мамандықтардың бірі бойынша академиялық магистр дәрежесі:

6М070300 – Ақпараттық жүйелер
6М100200 – Ақпараттық қауіпсіздік жүйелері
6М060200 – Информатика
6М011100 – Информатика
6М070200 – Автоматтандыру және басқару
6М070400 – Есептеуіш техника және программалық жабдықтау
6М060300 – Механика
6М070500 – Математикалық және компьютерлік модельдеу
6М060100 – Математика
6М071900 – Радиотехника, электроника и телекоммуникациялар

Тапсырушының мемлекеттік жоғары білім деңгейіне сай құжаты болуы керек.

«8D06301 – Ақпараттық қауіпсіздік жүйелері» мамандығы бойынша түсушілерге арналған емтихан бағдарламасы ақпараттық жүйелер кафедрасында жасалды.

3. Оқыту бағдарламасының пререквизиттері

Пререквизиттері:

1. Ақпараттық қауіпсіздік жүйелерін ұйымдастыру
2. Компьютерлік ақпаратты қорғаудың әдістері мен құралдары
3. Ақпаратты қорғау құралдарының элементтері

4. Емтихан тақырыптарының тізімі

«Ақпараттық қауіпсіздік жүйелерін ұйымдастыру» пәні

1. Классикалық шифрлар және оларды ашу. Ығыстыру және аффиндық шифрлар олардың дешифралу және теру (перебор) әдісімен ашу. Ауыстыру шифрын ашудың жиілікті әдісі.

Классикалық шифрлардың кемшіліктері, орыс және қазақ тіліндегі мәтіндердің жиілікті талдауы.

2. Бүтін сандар сақинасы, Евклид алгоритмы және салдарылары. Салыстыру теориясы. Модуль бойынша салыстурылардың қасиеттері. Модуль бойынша түрленетін элементтер.
3. Эйлер функциясы және оның қасиеттері. Жай сандардан Эйлер функциясының мәндері. Эйлер функциясының мультипликативтігі туралы теорема. Эйлер функциясының мәндерін табу формуласы. Эйлер функциясының көмегімен дәрежеге шығару.
4. Ферма-Эйлер теоремасы және RSA шифрдың негізгі теоремасы.
5. RSA-шифр, шифрлеу және оқу процестері, негіздемесі. Берілген мәтіннің ашық кілтімен RSA-шифрлеу. Берілген мәтіннің жабық кілтімен RSA-дешифрлеу.
6. RSA-электрндық қолтаңбасы, мәні және негіздеуі.
7. RSA-электрондық қолтаңба процедурасының жүзеге асырылуы, электрондық қолтаңбамен құжатқа қолтаңба қою бөлігі.
8. RSA-электрондық қолтаңба процедурасының жүзеге асырылуы, қолтаңбаны ашық кілтпен шифрлеу бөлігі.
9. Натурал сандар тізбегінде жай сандардың үлестірілуі және RSA шифрді бағалау.
10. $< F_2 ; +,* >$ өрісіндегі көпмүшеліктер сақинасы, Евклид алгоритмі, екі көпмүшеліктің ең үлкен ортақ бөлгішін көрсету. Осы сақинадағы келтірілмейтін көпмүшеліктер. 2,3,4,5 дәрежелі келтірілмейтін көпмүшеліктер.
11. $< F_2^n ; +,* >$ өрісін келтірілмейтін көпмүшеліктің модуль бойынша қалдықтарынан құралған өріс ретінде қалыптастырылуы. Осы өрістегі қосу және көбейту амалдары. Осы өрістің нөлдік емес элементтері үшін қосу бойынша және көбейту бойынша кері элементтер. $< F_{16} ; +, * >$ өрісін құрастыру.
12. Топ ретінің ішкі топ ретіне бөлінуі туралы Лагранж теоремасы. Элементтің реті топтың ретін бөлетіні туралы салдар. Z_n тобының ішкі топтарының мысалдары. $< F_{2n} ; +,* >$ өрісіндегі бастапқы элемент туралы теорема. $< F_{16} ; +,* >$ өрісінің бастапқы элементтері.
13. *n*-разрядті екілік блоктардан жасалған өрісінің құрылымы. Осы өрісте қосу мен көбейту амалдарын беру. Осы өрістің нөлдік емес элементтері үшін қосу және көбейту амалдары бойынша кері элементтер. 4-разрядты екілік блоктардан өрісті құру, осы өрістің бастапқы элементтерін көрсету.
14. Дифи-Хеллман есебі. Дифи-Хеллман есебінің «шешілмеушілігіне» сүйеніп, қашықтағы қолданушылар үшін ортақ құпияны құру. Қашықтағы қолданушылар үшін кілттер алмасу мәселесінің шешімі.
15. Эль-Гамаль шифры, кілттермен алмасу, шифрлеу және дешифрлеу процестері. Жүзеге асыру мысалы.

Қажетті әдебиеттер тізімі

Негізгі:

1. Яблонский С. В. Введение в дискретную математику. М.: Высшая школа, 2010. – 381 с.
2. Черёмушкин А. В. Лекции по арифметическим алгоритмам в криптографии. М.: МЦНМО, 2012.
3. Кормен Т., Лейзер Ч., Риверс Р. АЛГОРИТМЫ: построение и анализ. М.: МЦНМО, 2010. – 900 с.
4. А. П. Алферов т.б., Основы криптографии. Москва: «Гелиос АРВ», 2002 г.
5. В. И. Нечаев. ЭЛЕМЕНТЫ КРИПТОГРАФИИ. Основы защиты информации. М.: Высшая школа, 1999 г.

Қосымша:

1. А. А. Бухштаб. Основы теории чисел. М.: Просвещение, 1966.
2. D. R.Stinson. KRIPTOGRAPHY, Teory and Practice. CRC Press, Boca Raton, 1995.

«Компьютерлік ақпаратты қорғаудың әдістері мен құралдары» пәні

1. Криптология әдістерінің шығуы мен дамуы туралы қысқаша тарихи ақпарат. Криптография. Құпиялылық. Тұтастық. Аутентификация. Сандық қолтаңба.
2. Белл-Лападула моделі. Кілттердің алдын ала таратылуы. Кілттерді жіберу. Кілттерді ашық тарату. Құпияны бөлісу схемасы. Ашық кілттер инфрастуктурасы. Сертификаттар. Сертификациялау орталықтары. Шифрлердің формальді модельдері. Ашық мәтіндер модельдері. Ашық мәтіннің математикалық модельдері. Ашық мәтінді тану критерийлері. Шифрлерді әртүрлі көрсеткіштер бойынша жіктеу. Ауыстыру шифрінің математикалық моделі. Ауыстыру шифрлерін жіктеу.
3. Low-Water-Mark (LWM) моделі. Бағдарлық алмастырулар. Алмастыру шифрлерін криптоталдау элементтері. Ауыстыру шифрлері.
4. J. Goguen, J. Meseguer модельдері. Кестелік гаммалау. Гамма таңбаларының ықтималдықтарын қалпына келтіру мүмкіндігі туралы. Әртүрлі ықтималдықты гаммамен шифрленген мәтіндерді қалпына келтіру. Гамманы қайталап пайдалану. Виженер шифрін криптоталдау. Шифрлеушінің қателері.
5. Қауіпсіздіктің бұзылуын анықтау моделі. Энтропия және тіл артықтығы. Жалғыздық арақашықтығы. Шифрлердің беріктігі. Шифрлердің теориялық беріктігі. Шифрлердің практикалық беріктігі. Шифрлердің имитациялық беріктігі. Бұрмалауды таратпайтын шифрлер. «Таңбаларды ауыстыру» бұрмалауын таратпайтын шифрлер. «Таңбаларды тастап кету-кірістіру» бұрмалауын таратпайтын шифрлер.
6. Блоктық шифрлеу жүйелері. Блоктық шифрлерді құру принциптері. Блоктық шифрлер мысалдары. DES мәліметтерді шифрлеудің американдық стандарты. ГОСТ 28147-89 мәліметтерді шифрлеу стандарты. Блоктық шифрлерді пайдалану режимдері. Блоктық шифрлеу алгоритмдерін аралас пайдалану. Блоктық шифрлеу алгоритдерін талдау әдістері. Блоктық шифрлеу алгоритмдерін пайдалану бойынша ұсыныстар.
7. Шифрлеудің ағымдық жүйелері. Ағымдық шифржүйелерді синхронизациялау. Ағымдық шифржүйелерді құру принциптері. Ағымдық шифржүйелердің мысалдары. A5 шифржүйесі. Гиффорд шифржүйесі. Сызықтық ығыстыру регистрлері. Берлекемп-Месси алгоритмі. Сызықтық рекуррентті тізбектердің күрделенуі. Сүзгі генераторлар. Қиыстырушы генераторлар. Сызықтық ығыстыру регистрлерін композициялау. Рекурсия заңы динамикалық өзгеретін сұлбалар. Жады элементтері бар сұлбалар. Ағымдық шифрлерді талдау әдістері.
8. Қауіпсіздікті басқару. Стандарттар, қауіпсіздік аудиты. Сөйлеу сигналдарының ерекшеліктері. Скремблерлеу. Сигналдың жиілікті түрленулері. Сигналдық мерзімдік түрленулері. Мерзімдік алмастырулар жүйелерінің беріктігі. Сандық телефония жүйелері.
9. Ашық кілтті шифрлеу жүйелері. RSA шифржүйесі. Эль-Гамаль шифржүйесі. Мак-Элис шифржүйесі. "Рюкзак мәселесі" негізіндегі шифржүйе.
10. Идентификациялау. Құпия сөздерді құру ережелері. Құпия сөздерді тексеру рәсімдерін күрделендіру. Құпия тіркестер. Тиянақталған құпия сөздерге шабуыл. Құпия сөздерді қайталап пайдалану. Құпия сөздерді толықтай теріп шығу. Сөздік көмегімен шабуылдау. Жеке идентификациялау нөмірлері. Бір реттік құпия сөздер. “Сұрақ–жауап” (күшті идентификациялау). Симметриялық шифрлеу алгоритмдерін пайдаланып “сұрақ-жауапты” жүзеге асыру. Ассимметриялық шифрлеу алгоритмдерін пайдаланып “сұрақ-жауапты” жүзеге асыру. Нөлдік білімі бар хаттамалар. Идентификация хаттамаларына шабуыл.
11. Криптографиялық хеш функциялар. Хэштеу функциялары мен мәліметтер тұтастығы. Кілттік хэштеу функциялары. Кілтсіз хэштеу функциялары. Мәліметтердің тұтастығы және хабарлардың аутентификациясы. Хэштеу функцияларына ықтимал шабуылдар.
12. Сандық қолтаңбалар. Жалпы тұжырымдар. Ашық кілтті шифржүйелер негізіндегі сандық қолтаңбалар. Фиат–Шамир сандық қолтаңбасы, Эль-Гамаль сандық қолтаңбасы. Бір реттік сандық қолтаңбалар.

13. Кілттерді тарату хаттамалары. Симметриялық шифрлеуді пайдаланып кілттерді тапсыру. Екіжақты хаттамалар. Үштарапты хаттамалар. Асимметриялық шифрлеуды пайдаланып кілттерді тапсыру. Сандық қолтаңбаны пайдаланбайтын хаттамалар. Сандық қолтаңбаны пайдаланатын хаттамалар. Ашық кілт сертификаттары. Кілттерді ашық тарату. Кілттерді алдын ала тарату. Байланыс желісінде кілттерді алдын ала тарату схемалары. Құпия бөлісу схемалары. Конференцбайланысқа арналған кілттерді белгілеу әдістері. Кілттерді тарату хаттамаларына ықтимал шабуылдар.
14. Кілттерді басқару. Кілттердің өмірлік циклі. Сенімді үшінші тарап ұсынатын қызметтер. Уақыт белгілерін орнату. Сандық қолтаңбаларды нотаризациялау.
15. Шифржүйелерді пайдаланудың кейбір практикалық аспектілері. Хабарламалар ағымын талдау. Операторлар қателері. Шифржүйелерді пайдалану кезіндегі физикалық және ұйымдастырушылық іс-шаралар. Кілттерді ашық таратудың кванттық криптографиялық хаттамасы. Кванттық арна және оның қасиеттері. Кілттерді ашық тарату хаттамасы.

Қажетті әдебиеттер тізімі

Негізгі:

1. Акритас А. Основы компьютерной алгебры с приложениями. М.: Мир, 1994.
2. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2002. 2-е изд.
3. Берлекэмп Э. Алгебраическая теория кодирования. М.: Мир, 1971.
4. Василенко О.Н. Современные способы проверки простоты чисел. Обзор // Кибернетич. сборн. 1988. Вып. 25. С. 162-188.
5. Гашков С. Б. Упрощенное обоснование вероятностного теста Миллера-Рабина для проверки простоты чисел // Дискретная математика. 1998. Т. 10 (4). С. 35-38.
6. Дэвенпорт Дж., Сирэ И., Турнье Э. Компьютерная алгебра. М.: Мир, 1991.
7. Кнут Д. Искусство программирования. Т. 2. Получисленные алгоритмы. Вильямс: М.—СПб.-Киев, 2000. 3-е издание.
8. Кострикин А.И. Введение в алгебру. М.: Наука, 1977.
9. Нечаев В.И. Элементы криптографии. М.: Высшая школа, 1999.
10. Ноден П., Китте К. Алгебраическая алгоритмика. М.: Мир, 1999.
11. Панкратьев Е.В. Компьютерная алгебра. Факторизация многочленов. М.: Изд-во МГУ, 1988.

Қосымша:

1. Анохин М.И., Варновский Н.П., Сидельников В.М., Ященко В.В. Криптография в банковском деле. М.: МИФИ, 1997.
2. Виноградов И.М. Основы теории чисел. М.: Наука, 1972.
3. Гантмахер Ф. Р. Теория матриц. М., 1954.
4. Касселс Дж. Введение в геометрию чисел. М.: Мир, 1965.
5. Ленг С. Введение в теорию диофантовых приближений. М.: Мир, 1970.
6. Ленг С. Эллиптические функции. М.: Наука, 1984.
7. Чебышев П.Л. Полное собрание сочинений. Т. 1. Теория чисел. Изд-во АН СССР, 1946.
8. Чистов А.Л. Алгоритм полиномиальной сложности для разложения многочленов и нахождения компонент многообразия в субэкспоненциальное время // Зап. науч. семин. ЛОМИ АН СССР. 1984. №137. С. 124—188.

«Ақпаратты қорғау құралдарының элементтері» пәні

1. Компьютерлік жүйе (КЖ). Негізгі түсініктер. Электрондық құжат (ЭҚ). КЖ-гі ақпарат түрлері.
2. Компьютерлік жүйелердің осалдығы. Қол жеткізу, қол жеткізу субъектісі мен объектісі түсініктері. Рұқсатсыз қол жеткізу (РсҚЖ) туралы түсінік. РсҚЖ кластары және түрлері.
3. Компьютерлік жүйелердегі қауіпсіздік саясаты. Қауіпсіздік саясаты ұғымы және оның негізгі тұжырымдамасы. Қауіпсіздікті бағалау.

4. Мәліметтерге қол жеткізудің КЖ-субъектілерін қолданушыларды идентификациялау. Қолданушыны идентификациялау мәселесі. Идентификация хаттамасы ұғымы. Идентификациялаушы ақпарат ұғымы.
5. Файлдарға қолжетімділікті шектеу құралдары мен әдістері. РсҚЖ-ден мәліметтерді қорғаудың негізгі тәсілдері. Қол жеткізу фактілерін белгілеу әдістері. Қол жеткізу журналдары.
6. Процесс тарапынан мәліметтерге қатынасу. Мәліметтерді өзгертуден қорғау ерекшеліктері. Қол жеткізуді шектеу жүйелерінің сенімділігі. Хеш функцияны құруға негізделген әдіс, қойылатын талаптар және жүзеге асыру жолдары.
7. Программалық-аппараттық шифрлеу құралдары. Программалық-аппараттық шифрлеу кешендерін құру. Сигналдық процессорлардың негізінде криптотүрлендіру модульдерін жобалау.
8. ЭЕМ компоненттеріне қолжетімділікті шектеудің әдістері мен құралдары. ДЭЕМ компоненттері. ДЭЕМ қорғалатын компоненттерінің жіктелуі: ДЭЕМ-нің шеттетілетін және шеттетілмейтін компоненттері.
9. Программаларды рұқсатсыз көшіруден қорғау. Көшіруден қорғау мәселесіне көзқарас. Программалық жабдықтаманы көшіруден қорғаудың жалғыз құралы ретінде ПЖ-ны аппараттық ортаға және физикалық тасымалдаушыларға тәуелдендіруді пайдалану.
10. Маңызды ақпаратты сақтау. Құпия сөздер мен кілттер. Қатынасуды бақылау мақсатында қолданылатын құпия ақпарат: кілттер мен құпия сөздер.
11. Криптографиялық кілттерді басқару. Кілттерді генерациялау. Кілттерді тарату.
12. Симметриялық криптожүйелер үшін кілттерді таратуды аутентификациялау хаттамасы. Негізгі түсініктер мен анықтамалар, криптографиялық хаттамалардың типтері, мысалдар.
13. Асимметриялық криптожүйелерге арналған ашық кілттер сертификаттарын пайдаланатын хаттама.
14. Кілттерді сақтауды ұйымдастыру (жүзеге асыру мысалдары). Тікелей қолжетімді магниттік дискілер. TouchMemory құралы.
15. Программаларды оқып үйренуден қорғау. Программалық жабдықтаманы оқып үйрену және кері жобалау. ПЖ жұмысын зерделеудің мақсаты мен міндеттері. ПЖ зерделеу тәсілдері: статикалық және динамикалық зерделеу.

Қажетті әдебиеттер тізімі

<u>Негізгі:</u>

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тесты на языке Си. – М.: ТРИУМФ, 2003. – 816 с.
2. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах. – М.: ДМК Пресс, 2002. – 656 с. – (Сер. “Администрирование и защита”).
3. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2005.
4. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. М.: КУДИЦ-ОБРАЗ, 2003.
5. Столлингс В. Операционные системы. М.: Издательский дом «Вильямс», 2014. – 848 с.

<u>Қосымша:</u>

1. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд. – М.: Вильямс, 2001. – 672 с.
2. Нечаев В.И. Элементы криптографии (Основы теории защиты информации) / Под ред. В.А. Садовничего. – М.: Высшая школа, 1999. – 109 с.
3. Зубов А.Ю. Криптографические методы защиты информации. Совершенные шифры. М.: Гелиос АРВ, 2005.

4. Фороузан Б.А. Криптография и безопасность сетей: Учебное пособие / Фороузан Б.А.; перевод с англ. под ред. А.Н. Берлина. – М.: Интернет-Университет Информационных технологий: БИНОМ. Лаборатория знаний, 2010 – 784 с.

ЕМТИХАН ҚОРЫТЫНДЫСЫН БАҒАЛАУ ШКАЛАСЫ

Абитуриент өзінің ақпараттық қауіпсіздік жүйелерін ұйымдастыру принциптерін меңгергендігін, компьютерлік ақпаратты қорғау әдістері мен құралдарын, ақпаратты қорғау құралдарының элементтерін пайдалана білетіндігін, ақпараттық қауіпсіздік саласындағы қазіргі заманғы технологияларының дамуының негізгі жетістіктерін толық меңгергендігін көрсеткен жағдайда оған **«өте жақсы»** деген баға қойылады. Үміткер өзінің ойын толық әрі нақты жазбаша да ауызша жеткізе білуі; меңгерген білімін практикалық жүзеге асыра білуі; талқылай ойын қорытындылай білуі керек.

Абитуриент өзінің ақпараттық қауіпсіздік жүйелерін ұйымдастыру принциптерін жетік меңгергендігін, компьютерлік ақпаратты қорғау әдістері мен құралдарын, ақпаратты қорғау құралдарының элементтерін пайдалана білетіндігін, ақпараттық қауіпсіздік саласындағы қазіргі заманғы технологияларының дамуының негізгі жетістіктерін жетік меңгергендігін көрсеткен жағдайда оған **«жақсы»** деген баға қойылады. Үміткер өзінің ойын толық әрі нақты жазбаша да ауызша жеткізе білуі; меңгерген білімін практикалық жүзеге асыра білуі; талқылай ойын қорытындылай білуі тиіс.

Абитуриент өзінің ақпараттық қауіпсіздік жүйелерін ұйымдастыру принциптерін әлсіз меңгергендігін, компьютерлік ақпаратты қорғау әдістері мен құралдарын, ақпаратты қорғау құралдарының элементтерін пайдалана білетіндігін, ақпараттық қауіпсіздік саласындағы қазіргі заманғы технологияларының дамуының негізгі жетістіктерін жеткіліксіз меңгергендігін көрсеткен жағдайда оған **«қанағаттанарлық»** деген баға қойылады. Үміткер өзінің ойын толық әрі нақты жазбаша да ауызша жеткізе білмейді; меңгерген білімін практикалық жүзеге асыра білу; талқылай ойын қорытындылай білу керек.

Абитуриент өзінің ақпараттық қауіпсіздік жүйелерін ұйымдастыру принциптерін меңгермегендігін, компьютерлік ақпаратты қорғау әдістері мен құралдарын, ақпаратты қорғау құралдарының элементтерін пайдалана білмейтіндігін, ақпараттық қауіпсіздік саласындағы қазіргі заманғы технологияларының дамуының негізгі жетістіктерін меңгермегендігін көрсеткен жағдайда оған «**қанағаттанарлықсыз**» деген баға қойылады. Үміткер өзінің ойын толық әрі нақты жазбаша да ауызша жеткізе білмейді; меңгерген білімін практикалық жүзеге асыра білмейді; талқылай ойын қорытындылай білмейді.