5А330301 – Криптография ва криптоанализ мутахассислиги бўйича магистратурага кирувчилар учун имтиҳон саволлар

Ахборот хавфсизлиги фани

1. Миллий хавфсизлик тушунчаси.
2. Ахборот хавфсизлигини таъминлашнинг асосий вазифалари ва даражалари.
3. Хавфсизлик сиёсати.
4. Ахборот хавфсизлиги архитектураси ва стратегияси.
5. Ахборот хавфсизлигига таҳдидлар ва уларнинг таҳлили.
6. Ахборот хавфсизлигининг заифликлари.
7. Ахборотнинг маҳфийлигини, яхлитлигини ва фойдаланувчанлигини бузиш усуллари.
8. Ахборот хавфсизлиги соҳасига оид ҳалқаро стандартлар
9. Ахборот хавфсизлиги соҳасига оид миллий стандартлар
10. Ахборот хавфсизлиги соҳасига оид меьёрий хужжатлар
11. Хавфсизлик моделлари. Харрисон-Руззо-Улманнинг дискрецион модели.
12. Хавфсизлик моделлари. Белла-ЛаПадуланинг мандатли модели.
13. Хавфсизлик моделлари. Хавфсизликнинг ролли модели.
14. Шифрлаш усуллари.
15. Симметрик шифрлаш тизимлари.
16. Асимметрик шифрлаш тизимлари.
17. Хэшлаш функцияси.
18. Электрон рақамли имзо.
19. Стеганография.
20. Криптотаҳлил усуллари.
21. Идентификация ва аутентификация тушунчаси.
22. Пароллар асосида аутентификациялаш.
23. Сертификатлар асосида аутентификациялаш.
24. Қатъий аутентификациялаш.
25. Фойдаланувчиларни биометрик идентификациялаш ва аутентификациялаш.
26. Компьютер вируслари ва вирусдан ҳимояланиш муаммолари.
27. Вирусга қарши дастурлар.
28. Вирусга қарши ҳимоя тизимини қуриш.
29. Тармоқлараро экранларнинг ишлаш хусусиятлари.
30. Тармоқлараро экранларнинг асосий компонентлари.
31. Тармоқлараро экранлар асосидаги тармоқ ҳимоясининг схемалари.
32. Виртуал ҳимояланган тармоқларни қуриш концепцияси. VPN тармоқнинг асосий тушунча ва функциялари.
33. Виртуал ҳимояланган тармоқларни қуриш концепцияси. Виртуал ҳимояланган каналларни қуриш вариантлари
34. Симсиз алоқа тизимларида ахборот ҳимояси.
35. Операцион тизим хавфсизлигини таъминлаш муаммолари.
36. Операцион тизимни ҳимоялаш қисмтизимининг архитектураси.
37. Ахборотни ҳимоялашда дастурий иловаларнинг қўлланилиши.
38. Ахборот сирқиб чиқадиган техник каналлар ва уларнинг туркумланиши.
39. Ахборот сирқиб чиқадиган техник каналларни аниқлаш усуллари ва воситалари.
40. Объектларни инженер химоялаш ва техник қўриқлаш.

“Маълумотлар базаси хавфсизлиги” фани

1. Маълумотлар базаси хавфсизлигини таъминлаш усуллари, воситалари ва механизмларининг асосий характеристикалари.
2. Маълумотлар базасини бошқариш тизимларининг турлари.
3. Маълумотлар базаси хавфсизлигининг технологик жиҳатлари.
4. Маълумотлар базасида идентификация ва аутентификация технологиялари.
5. Маълумотлар базаси хавфсизлиги тиллари.
6. Маълумотлар базасида объектлардан такроран фойдаланиш хавфсизлигини таъминлаш технологиялари.
7. Маълумотлар базасида ишончли лойиҳалаш ва маъмурлаш технологиялари
8. Маълумотлар базаси хавфсизлиги моделлари.
9. Дискрецион модел асосида маълумотлар базасидан фойдаланишни чеклашни ташкил этиш.
10. Белл-ЛаПадула модели асосида маълумотлар базасидан фойдаланишни чеклашни ташкил этиш.
11. Мандатли модел асосида маълумотлар базасидан фойдаланишни чеклашни ташкил этиш.
12. Ролли модел асосида маълумотлар базасидан фойдаланишни чеклашни ташкил этиш.
13. Маълумотлар базасида аудитлаш ва администрациялаш.
14. Маълумотлар базасининг тақсимланган тизимида ахборот хавфсизлиги консепцияси.
15. Марказлаштирилган кўпчилик фойдаланувчи ахборот тизимларида маълумотлар базаси хавфсизлиги.
16. Маълумотлар базасида маълумотларни объектли боғлаш технологияси.
17. Маълумотлар базасини бошқариш тизимларида хавфсизлик аудитини ўтказиш хусусиятлари.
18. Маълумотлар базасини тиклаш.
19. Маълумотлар базасини бошқаришнинг замонавий тизимларида репликасияни синхронлаш жараёни.
20. Маълумотлар базаси хавфсизлиги қисмтизимининг архитектураси ва ишлаш принципи.
21. Маълумотлар базасини бошқариш тизимларининг химоя профиллари.
22. Маълумотлар базаси хавфсизлигини таъминлашдаги меъёрий хужжатлар.
23. Маълумотлар базасида руҳсатларни бошқариш технологиялари.
24. Маълумотлар базасида авторизация ва маъмурлаш жараёнлари.
25. MSSQL МББТнинг ҳимоялаш параметрлари.
26. Oracle МББТнинг ҳимоялаш параметрлари.
27. Маълумотлар базасида SQL инъекция хужумлари ва уларни олдини олиш усуллари.
28. Захира нусхалаш усуллари ва RAID контроллерлари.
29. Маълумотлар базасида “Мижоз-сервер” технологияси.
30. Маълумотлар базасини репликациялаш усуллари.

“Криптография усуллари” фани

1. Ахборотни ҳимоялашда криптографиянинг ўрни.
2. Криптотизмларга қўйиладиган талаблар. Кирхгоф принципи.
3. Криптографик тизимларда бардошлилик тушунчаси. Назарий, амалий бардошлилик.
4. Модуль арифметикаси хусусиятлари.
5. Энигма машинаси ва унда калит ўлчами.
6. Шифрлаш усулларининг классификацияси.
7. Классик шифрлаш усуллари ва уларда фойдаланилган акслантиришлар.
8. Классик шифрлаш усулларининг криптотаҳлили (Цезер, Аффин тизимидаги Цезер, Сеҳрли квадрат, Вижинер, Икки томонлама ўрин алмаштириш, Гамилтон маршрути).
9. Симметрик шифрлаш усуллари. Блокли ва оқимли симметрик шифрлаш усуллари.
10. Блокли симметрик шифрларни яратишда Фейстел, SP ва Лаи-Массей тармоғларидан фойдаланиш.
11. Симметрик блокли шифрлаш алгоритмларининг шифрлаш режимлари.
12. DES шифрлаш стандарти ва унинг криптотаҳлили.
13. ГОСТ 28147-89 блокли шифрлаш стандарти ва унинг криптотаҳлили.
14. AES шифрлаш стандарти ва унинг криптотаҳлили.
15. Оқимли шифрлаш алгоритмларнинг моҳияти. Псевдотасодифий ва тасодифий сонлар генератори.
16. A5/1 оқимли шифрлаш алгоритми ва унинг криптотаҳлили.
17. RC4 оқимли шифрлаш алгоритми ва унинг криптотаҳлили.
18. Очиқ калитли шифрлаш алгоритмлари ва уларни яратишда фойдаланилган математик муаммолар.
19. Симметрик ва очиқ калитли шифрлаш тизимларининг қиёсий таҳлили.
20. Катта сонларни туб кўпайтувчиларга ажратиш муаммоси. RSA алгоритми ва унинг таҳлили
21. Дискрет логарифмлаш муаммоси. Эл - Гамал алгоритми ва унинг таҳлили.
22. Эллиптик эрги чизиқ муаммоси ва ундан очиқ калитли криптотизимларни яратишда фойдаланиш.
23. Хэш функциялар ва уни ахборотни ҳимоялашдаги ўрни.
24. MD5 хэш функцияси ва унинг таҳлили.
25. Калитли хэш функциялар. MAC тизимлари.
26. Электрон рақамли имзо тизимлари ва уларнинг асосий вазифалари.
27. RSA ва Эл-Гамалга асосланган ЭРИ алгоритмлари.

По предмету Информационная безопасность

1. Понятие национальной безопасности.
2. Основные задачи и уровни обеспечения информационной безопасности.
3. Политика безопасности
4. Архитектура и стратегии информационной безопасности.
5. Угрозы информационной безопасности и их анализ.
6. Уязвимости информационной безопасности.
7. Методы нарушения конфиденциальности, целостности и доступности информации .
8. Международные стандарты в сфере информационной безопасности.
9. Национальные стандарты в сфере информационной безопасности.
10. Нормативные документы в сфере информационной безопасности.
11. Модели безопасности. Дискреционная модель Хоррисона-Руззо-Ульмана.
12. Модели безопасности. Мандатная модель Белла-ЛаПадулы.
13. Модели безопасности. Ролевая модель безопасности.
14. Методы шифрования.
15. Симметричные системы шифрования.
16. Асимметричные системы шифрования.
17. Функция Хеширования.
18. Электронная цифровая подпись.
19. Стеганография.
20. Методы криптоанализа.
21. Понятие идентификации и аутентификации.
22. Аутентификация на основе паролей.
23. Аутентификация на основе на основе сертификатов.
24. Строгая аутентификация .
25. Биометрическая идентификация и аутентификация пользователей.
26. Компьютерные вирусы и проблемы защиты от вирусов.
27. Антивирусные программы.
28. Построение антивирусные системы защиты.
29. Особенности функционирования межсетевых экранов.
30. Основные компоненты межсетевых экранов.
31. Схемы защиты сети на основе межсетевых экранов.
32. Концепция построения виртуальных защищенных сетей VPN. Основные понятия и функции сети VPN.
33. Концепция построения виртуальных защищенных сетей VPN. Варианты построения виртуальных защищенных каналов.
34. Зашита информации в системах беспроводных сетях.
35. Проблемы обеспечения безопасности операционной системы
36. Архитектура подсистемы защиты операционной системы.
37. Применение программных приложений в защите информации.
38. Технические каналы утечки информации и их классификация
39. Методы и средства определения технических каналов утечки информации.
40. Инженерная защита и техническая охрана объектов .

По предмету Безопасность базы данных

1. Основные характеристики методов, средств и механизмов обеспечения безопасности базы данных.
2. Виды систем управления базами данных.
3. Технологические аспекты информационной безопасности базы данных.
4. Технологии идентификации и аутентификации в базе данных.
5. Языки безопасности базы данных.
6. Технологии обеспечения безопасности повторного использования объектов в базе данных.
7. Технология надежного проектирования и администрирования в базе данных.
8. Модели безопасности базы данных.
9. Организация разграничения доступа в базы данных на основе дискреционной модели.
10. Организация разграничения доступа в базы данных на основе модели Белл-ЛаПадулой.
11. Организация разграничения доступа в базы данных на основе мандатной модели.
12. Организация разграничения доступа в базы данных на основе ролевой модели.
13. Аудит и администрация в базе данных.
14. Концепция информационной безопасности в распределенных системах базы данных.
15. Безопасность базы данных в централизованных многопользовательських информационных системах.
16. Технология объектного связывания данных в базе данных.
17. Особенности проведения аудита безопасности в системах управления базами данных.
18. Восстановление базы данных.
19. Процесс синхронизаций репликации в современных системах управления базами данных.
20. Архитектура и принцип функционирования подсистемы безопасности базы данных.
21. Профили защиты систем управления базами данных.
22. Нормативные документы в области обеспечения безопасности базы данных.
23. Технология разграничения доступа в базе данных.
24. Процессы авторизация и администрация в базе данных.
25. Параметры защиты СУБД MSSQL.
26. Параметры защиты СУБД Oracle.
27. SQL инъекция в базе данных и методы предотвращения от них.
28. Методы резервного копирования и RAID контроллеры.
29. Технология «Клиент-сервер» в базе данных.
30. Методы репликации баз данных.

По предмету Криптографические методы

1. Роль криптографии в защиты информации.
2. Требования криптосистемам. Принцип Кирхгофа.
3. Понятие устойчивости в криптографических системах. Теоритическая, практическая устойчивость.
4. Характеристики модульной арифметики.
5. Машина Энигмы и размер ключа.
6. Классификация методов шифрования.
7. Классические методы шифрования и использованные преобразование в них.
8. Криптоанализ классических методов шифрования. (Цезар, Аффин, Магический квадрат, Вижинер, Метод двойной переустановки, Маршрут Гамильтона)
9. Симметричные методы шифрования. Блочные и поточные методы шифрования.
10. Использование сетей Фейстел, SP и Лаи-Массей при создание блочного симметричного шифрования.
11. Режимы алгоритмов симметричного блочного шифрования.
12. Стандарт алгоритма шифрования DES и его криптоанализ.
13. Стандарт алгоритма блочного шифрования ГОСТ 28147-89 и его криптоанализ.
14. Стандарт алгоритма шифрования AES и его криптоанализ.
15. Суть поточных алгоритмов шифрования. Генератор псевдослучайных и случайных чисел.
16. Алгоритм поточного шифрования A5/1 и его криптоанализ.
17. Алгоритм поточного шифрования RC4 и его криптоанализ.
18. Алгоритмы ассиметричного шифрования и использованные математических проблем в них.
19. Анализ симметричных и ассиметричных систем шифрования.
20. Проблема факторизации больших чисел. Алгоритм RSA и его криптоанализ.
21. Проблема дискретного логарифма. Алгоритм Эл - Гамал и его криптоанализ.
22. Проблема эллиптических кривых и использование при создание криптосистем открытого ключа.
23. Хэш-функции и роль в защиты информации.
24. Хэш-функции MD5 и его криптоанализ.
25. Ключевые хэш-функции. Системы MAC.
26. Системы электронных цифровых подписей и основные задачи.
27. ЭЦП основанный на RSA и Эл-Гамал.

Асосий адабиётлар

1. Ўзбекистон Республикаси Президенти Шавкат Мирзиёевнинг 2017 йил 7 февральдаги “Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегияси тўғрисида”ги ПФ-4947-сонли фармони.
2. Ўзбекистон Республикаси Президенти Шавкат Мирзиёевнинг “Танқидий таҳлил, қатъий тартиб-интизом ва шахсий жавобгарлик – ҳар бир раҳбар фаолиятининг кундалик қоидаси бўлиши керак”, Тошкент, “Ўзбекистон” 2017-йил.
3. Ўзбекистон Республикаси «Алоқа тўғрисида» Қонуни 13.01.1992й.
4. Ўзбекистон Республикаси “Ахборотлаштириш тўғрисида” Қонуни 2003й.
5. Каримов И.А. “Ўзбекистоннинг 20 йиллик тараққиёт йўли.” Президент И.А.Каримовнинг Ўзбекистон Республикаси Олий мажлиси, Вазирлар Маҳкамаси ва Президент Девонининг Ўзбекистон мустақиллигининг 20 йиллигига бағишланган қўшма мажлисидаги маърузаси. Халқ сўзи, 2011й.
6. Каримов И.А. “Инсон манфаатлари устиворлигини таъминлаш –барча ислоҳот ва ўзгаришларимизнинг бош мақсадидир”. Халқ сўзи газетаси. 2008 йил, 9 феврал.
7. Бройдо В.Л. Архитектура ЭВМ и систем. Учебник для вузов.- СПб. Питер. 2009.- 720 с.
8. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Учебник. –СПб. Питер. 2005г.
9. Ватаманюк А. Создание, обслуживание и администрирование сетей. СПб. Питер. 2010 – 282 с.
10. Шмидский Я.К. Программирование на языке С++: Самоучитель. Учебное пособие. Диалектика. 361 стр, 2004 г.
11. Л.К. Бабенко, Е.А. Ищукова. Современные алгоритмы блочного шифрования и методы их анализа: учеб.пособие для студентов вузов, обучающихся по группе специальностей в области информационной безопасности. – М.: Гелиос АРВ, 2006. -376с.,
12. Х.П. Хасанов. Такомиллашган диаматрицалар алгебралари ва параметрли алгебра асосида криптотизимлар яратиш усуллари ва алгоритмлари. Тошкент, 2008, -208 б.
13. Д.Е. Акбаров. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши. – Тошкент, “Ўзбекистон маркаси” нашриёти, 2009, - 432б.
14. Чирилло Дж. Защита от хакеров. (+CD). – СПб: Питер, 2003. – 480 с.:
15. Платонов В.В. Программно-аппаратные средства защиты информации. Учебное пособие для ВУЗов. –М.: Издательский центр «АКАДЕМИЯ», 2013.
16. С.К.Ганиев, М.М. Каримов, К.А.Ташев. Ахборот хавфсизлиги. Дарслик. Тошкент-“Фан ва технология”-2016.
17. С.К.Ганиев, А.А.Ганиев, Д.Я.Иргашева. Маълумотлар базаси хавфсизлиги. Тошкент-“Фан ва технология”-2016.
18. Борисов М.А.,Романов О.А. Основы организационно-правовой защиты информации. Изд.4-е-М.:Ленанд,2015.
19. Шаньгин В.Ф. Информационная безопасность.-М.:ДМК Пресс,2014.
20. Мельников Д.А. Информационная безопасность открытых систем: учебник/-М.:Флинта:Наука,2013.
21. Акбаров Д. Е. “Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши” – Тошкент, 2008 – 394 бет.
22. Stamp Mark. Information security: principles and practice. USA, 2011.
23. С.К.Ғаниев, М.М. Каримов. Ҳисоблаш системалари ва тармоқларида информация ҳимояси. Олий ўқув юрт.талаб. учун ўқув қўлланма.-Тошкент Давлат техника университети, 2003.
24. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: издательство ТРИУМФ, 2003 -816 стр.