Подписано электронной подписью:
Вержицкий Данил Григорьевич
Должность: Директор КГПИ ФГБОУ ВО «КемГУ»
Дата и время: 2024-02-21 00:00:00
471086fad29a3b30e244c728abc3661ab35c9d50210dcf0e75e03a5b6fdf6436

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Кемеровский государственный университет»

Новокузнецкий институт (филиал)

федерального государственного бюджетного образовательного учреждения

высшего образования

«Кемеровский государственный университет»

Физико-математический и технолого-экономический факультет

УТВЕРЖДАЮ
Декан ФМ и ТЭФ
_____ И.И. Тимченко
«24» марта 2017г.

Рабочая программа дисциплины
Б1.В.ДВ.19.1 Методы и средства защиты информации

Направление подготовки
44.03.05 Педагогическое образование (с двумя профилями подготовки)

Направленность (профиль) подготовки
Физика и информатика

Программа академического бакалавриата

Квалификация выпускника
бакалавр

Форма обучения
очная

Год набора 2013

Новокузнецк 2017

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы 44.03.05 Педагогическое образование (с двумя профилями подготовки) 3
2. Место дисциплины в структуре основной профессиональной образовательной программы бакалавриата 3
3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся 4
3.1. Объём дисциплины по видам учебных занятий (в часах) 4
4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий 4
4.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах) 4
4.2 Содержание дисциплины, структурированное по темам (разделам) 5
5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине 6
6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине 7
6.1. Паспорт фонда оценочных средств по дисциплине 7
6.2. Типовые контрольные задания или иные материалы 7
6.2.1. Экзаменационный тест 7
7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины 11
а) основная учебная литература: 11
б) дополнительная учебная литература: 11
8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины 11
9. Методические указания для обучающихся по освоению дисциплины 12
10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости) 13
11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине 13
12. Иные сведения и (или) материалы 14
12.1. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья 14
10.1. Перечень образовательных технологий, используемых при осуществлении образовательного процесса по дисциплине 14
10.2. Занятия, проводимые в интерактивных формах 14

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы 44.03.05 Педагогическое образование (с двумя профилями подготовки)

В результате освоения ОПОП бакалавриата обучающийся должен овладеть следующими результатами обучения по дисциплине:

Коды компетенции	Результаты освоения ОПОП Содержание компетенций	Перечень планируемых результатов обучения по дисциплине
ОК-7	способность использовать базовые правовые знания в различных сферах деятельности	Знать: основы правовых знаний; базовые нормативные документы в сфере образования. Уметь использовать нормативные правовые документы в своей деятельности. Владеть базовыми правовыми знаниями в различных сферах деятельности и применять знания основных нормативных документов в сфере образования
ОПК-4	готовность к профессиональной деятельности в соответствии с нормативно-правовыми документами сферы образования	Знать основы трудового законодательства, Конвенцию о правах ребенка, законы в сфере образования и федеральные государственные образовательные стандарты общего образования; приоритетные направления развития образовательной системы Российской Федерации; нормативных документов по вопросам обучения и воспитания детей и молодежи; нормативные правовые, руководящие и инструктивные документы, регулирующие организацию и проведение мероприятий за пределами территории образовательной организации (экскурсий, походов и экспедиций). Уметь использовать знания трудового законодательства, Конвенцию о правах ребенка, законы в сфере образования и федеральных государственных образовательных стандартов общего образования; применять знания направлений развития образовательной системы Российской Федерации; руководствоваться нормативными документами по вопросам обучения и воспитания детей и молодежи. Владеть способами организации профессиональной деятельности в соответствии нормативно-правовыми документами сферы образования; нормативными документами по вопросам обучения и воспитания детей и молодежи.

2. Место дисциплины в структуре основной профессиональной образовательной программы бакалавриата

Данная дисциплина относится к вариативной части блока дисциплин Б1 основной профессиональной образовательной программы подготовки бакалавров направления 44.03.05 «Педагогическое образование (с двумя профилями подготовки)» и является дисциплиной по выбору.

Для освоения дисциплины «Методы и средства защиты информации» студенты используют знания, умения, навыки, сформированные в процессе изучения студентами математических и информационно-технологических дисциплин, а также практический опыт работы с вычислительной техникой.

Дисциплина изучается на 5 курсе в А семестре.

3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 3 зачетных единиц (ЗЕТ), 108 академических часа.

3.1. Объём дисциплины по видам учебных занятий (в часах)

Объём дисциплины	Всего часов
Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	78
Аудиторная работа (всего):	42
в т. числе:	
Лекции	14
Семинары, практические занятия	
Практикумы	
Лабораторные работы	28
В т.ч. в активной и интерактивной форме	14
Внеаудиторная работа (всего):	30
В том числе, индивидуальная работа обучающихся с преподавателем:	
Курсовое проектирование	
Групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем	
Творческая работа (эссе)	
Самостоятельная работа обучающихся (всего)	30
Вид промежуточной аттестации обучающегося (зачет / экзамен)	экзамен

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах)

№ п/п	Раздел дисциплины	Общая трудоёмкость (в	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах)			Формы текущего контроля успеваемости
			аудиторные учебные занятия		самостоя-тельная работа обучаю-щихся	
		всего	лекции	лабораторные работы		
1.	Основные понятия информационной безопасности систем. Источники атак на информацию, риски.	10	2	4	4	Устный опрос, лабораторная работа
2.	Политика безопасности. Стандарты безопасности.	10	2	4	4	Устный опрос, лабораторная работа

№ п/п	Раздел дисциплины	Общая трудоёмкость (в	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах)			Формы текущего контроля успеваемости
			аудиторные учебные занятия		самостоя-тельная работа обучаю-щихся	
		всего	лекции	лабораторные работы		
3.	Криптографические модели. Алгоритмы шифрования.	10	2	4	4	Тест, лабораторная работа
4.	Модели безопасности основных ОС.	10	2	4	4	Тест, лабораторная работа
5.	Алгоритмы аутентификации пользователей.	10	2	4	4	Тест, лабораторная работа
6.	Многоуровневая защита корпоративных сетей.	10	2	4	4	Тест, лабораторная работа
7.	Защита информации в сетях. Требования к системам защиты информации.	12	2	4	6	Тест, лабораторная работа
	Итого:	**108**	**14**	**28**	**30**	**36**

4.2 Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Наименование раздела дисциплины	Содержание
Содержание лекционного курса		
1	Основные понятия информационной безопасности систем. Источники атак на информацию, риски.	Основные понятия информационной безопасности (ИБ) систем. Источники, риски и формы атак на информацию. Международные стандарты информационного обмена. Понятие угрозы. Необходимость защиты информационных систем и телекоммуникаций. Основные задачи обеспечения защиты информации.
2	Политика безопасности. Стандарты безопасности.	Политика безопасности. Стандарты безопасности. Анализ угроз ИБ. Классификация видов угроз ИБ по различным признакам. Свойства информации: конфиденциальность, доступность, целостность. Угроза раскрытия параметров системы, угроза нарушения конфиденциальности, угроза нарушения целостности, угроза отказа служб. Примеры реализации угроз ИБ.
3	Криптографические модели. Алгоритмы шифрования.	Криптографические модели. Алгоритмы шифрования.
4	Модели безопасности основных ОС.	Модели безопасности основных ОС. Особенности современных информационных систем, факторы влияющие на безопасность информационной системы. Понятие информационного сервиса безопасности. Виды сервисов безопасности. Идентификация и аутентификация. Парольные схемы аутентификации. Симметричные схемы аутентификации субъекта. Несимметричные схемы аутентификации (с открытым ключом).

№ п/п	Наименование раздела дисциплины	Содержание
5	Алгоритмы аутентификации пользователей.	Алгоритмы аутентификации пользователей. Использование криптографических средств для решения задач идентификация и аутентификация. Электронная цифровая подпись (ЭЦП), принципы ее формирования и использования. Подтверждение подлинности объектов и субъектов информационной системы.
6	Многоуровневая защита корпоративных сетей.	Многоуровневая защита корпоративных сетей. Основные нормативные руководящие документы, нормативно-справочные документы. Задачи в сфере обеспечения информационной безопасности на уровне государства. Особенности сертификации и стандартизации криптографических услуг. Законодательная база информационной безопасности. Концепция информационной безопасности.
7	Защита информации в сетях. Требования к системам защиты информации	Защита информации в сетях. Критерии безопасности компьютерных систем министерства обороны США (“Оранжевая книга”). Базовые требования безопасности: требования политики безопасности, требования подотчетности (аудита), требования корректности. Классы защищенности компьютерных систем. Интерпретация и развитие Критериев безопасности. Требования к системам защиты информации. Иерархический метод разработки защищенных систем. Структурный принцип. Принцип модульного программирования. Исследование корректности реализации и верификации автоматизированных систем. Спецификация требований предъявляемых к системе. Основные этапы разработки защищенной системы.
Темы лабораторных занятий		
1	Криптографические методы защиты.	Реализация криптографического преобразования информации по одному из доступных алгоритмов.
2	Алгоритмы аутентификации пользователей.	Изучение принципов аутентификации пользователей веб-сервисов.
3	Модели безопасности основных ОС.	Определение наличия и удаление вредоносного ПО с помощью программных средств антивирусного ПО.
4	Многоуровневая защита корпоративных сетей.	Исследование механизмов парольной защиты, методов противодействия атакам на пароль.
5	Защита информации в сетях.	Управление правами доступа к ресурсам ОС, ИС и веб-сервисов.
6	Требования к системам защиты информации.	Развертывание веб-сервера. Настройка параметров безопасности. Испытания эффективности его защиты.

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Темы для рефератов:

1. Вредоносное ПО: способы распространения, опасность, методы защиты.
2. Программные закладки: типы, способы внедрения и защиты.
3. Аппаратные средства защиты информации.
4. Сравнительный анализ средств защиты электронной почты.
5. Сравнительный анализ систем обнаружения атак.
6. Сравнительный анализ межсетевых экранов.
7. Анализ методов изучения поведения нарушителей безопасности компьютерных систем.
8. Анализ методов нарушения безопасности сетевых ОС и методов

противодействия им.

9. Применение биометрической информации для аутентификации пользователей компьютерных систем.

10. Стандарты безопасности компьютерных систем и информационных технологий.

11. Сравнительный анализ методов и программных средств защиты от спама.

12. Методы и программные средства перехвата и анализа контента.

13. Уязвимости симметричных и асимметричных криптографических систем.

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

6.1. Паспорт фонда оценочных средств по дисциплине

№ п/п	Контролируемые разделы (темы) дисциплины (результаты по разделам)	Код контролируемой компетенции	наименование оценочного средства
1.	Методы защиты информации	ОК-7, ОПК-4	Тест
2.	Требования к системам защиты информации.	ОК-7, ОПК-4	Тест
3.	Модели безопасности основных ОС. Алгоритмы аутентификации пользователей.	ОК-7, ОПК-4	Тест

6.2. Типовые контрольные задания или иные материалы

6.2.1. Экзаменационный тест

1. Укажите три основные угрозы для информации в человеко-компьютерных системах:

a. Резервное копирование
b. Сбои оборудования
c. Протоколирование состояния системы
d. Случайная утрата или изменение
e. Преднамеренное искажение
f. Санкционированный просмотр

2. В эталонной модели OSI, шифрование входит в функции уровня...

a. Канального (2)
b. Сетевого (3)
c. Сеансового (5)
d. Представления (6)
e. Транспортного (4)
f. Физического (1)
g. Приложений (7)

3. Вредоносный код обладает следующими чертами: не требует программы-носителя, самовоспроизводится и размножается по сети без ведома пользователя, заражая другие компьютеры. Его тип -

a. Червь
b. Троянский конь
c. Файловый вирус
d. Макровирус

4. Наиболее опасной из приведенных процедур восстановления забытого пароля является...

a. пересылка текущего пароля на адрес электронной почты, при этом адрес заполняется автоматически из профиля заявителя

b. пересылка на адрес электронной почты, связанной с профилем, ссылки на процедуру восстановления пароля, имеющую ограниченный срок актуальности

c. пересылка текущего пароля на адрес электронной почты, при этом адрес и логин указывается вручную заявителем

d. генерация нового пароля и его пересылка на адрес электронной почты, указанной в профиле заявителя

5. Межсетевые экраны служат для

a. Изоляции некоторой сети от других с помощью настраиваемых фильтров трафика и/или анализаторов угроз

b. сбора статистики использования каналов связи сотрудниками организации

c. Для просмотра информации, распределенной по узлам нескольких сетей

d. подтверждения подлинности сообщений, принятых по сети

e. отображения

6. Криптосистема обладает следующими чертами: предусматривает использование открытого ключа для шифрования и закрытого для дешифрования данных. Тип криптосистемы -

a. Избыточная

b. Симметричная

c. Асиметричная

d. С использованием инфраструктуры открытых ключей (PKI)

7. Среди методов защиты информации от ошибочных действий пользователей можно выделить три наиболее эффективных:

a. Резервирование носителей информации

b. Автоматический запрос на подтверждение выполнения команды или операции

c. Шифрование файлов

d. Предоставление возможности отмены последнего действия

e. Установление специальных атрибутов файлов

f. Отчет о действиях пользователя

8. Под целостностью в контексте информационной безопасности понимают

a. возможность за приемлемое время получить требуемую информационную услугу

b. актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения

c. полноту предоставляемых данных по теме запроса

d. комплексный подход к обеспечению информационной безопасности

9. Наиболее частыми и опасными угрозами ИБ являются

a. непреднамеренные ошибки штатных пользователей, операторов или администраторов ИС

b. хакерские атаки

c. сбои аппаратного обеспечения и поддерживающей инфраструктуры

d. стихийные бедствия, забастовки, войны

10. Протокол удаленного администрирования, аналогичный Telnet, но

обеспечивающий шифрование потока данных, а также различные варианты аутентификации:

a. SSH
b. VPN
c. RDP
d. TLS
e. SSL

11. Три наиболее важных метода защиты информации от несанкционированного доступа:

a. Архивирование (создание резервных копий)
b. Регулярное обновление аппаратных средств
c. Шифрование информации
d. Установка паролей на доступ к информации
e. Использование антивирусных программ

12. Окном опасности называют

a. диалоговое окно ОС или антивирусной программы с предупреждением об опасности
b. средства, используемые злоумышленниками для установки средств удаленного управления компьютером
c. уязвимости в защите ПО или ИС, позволяющие создать угрозу информационной безопасности
d. промежуток времени от момента, когда появляется возможность использовать уязвимость в защите, и до момента, когда она ликвидируется

13. Согласно стандарту Министерства обороны США "Критерии оценки доверенных компьютерных систем" (известным под названием "Оранжевая книга") степень доверия системе оценивается по двум основным критериям:

a. Степень квалификации пользователей
b. Стоимость систем обеспечения безопасности
c. Политика безопасности
d. Уровень гарантированности
e. Квалификации сотрудников физической охраны

14. Электронная цифровая подпись (ЭЦП) ...

a. это подпись под сообщением или документом, включающая контакты отправителя
b. ставится на сенсорном экране
c. применяется только для обмена служебными документами, но не личной информацией
d. предназначена для защиты электронного документа от подделки
e. это скан рукописной личной подписи

15. Монитор обращений ("ядро безопасности") должен обладать как минимум тремя важными характеристиками:

a. Документированность
b. Изолированность
c. Полнота
d. Прозрачность

e. Верифицируемость

16. Криптосистема обладает следующими чертами: предусматривает использование одного и того же закрытого ключа для шифрования и дешифрования данных, характеризуется высокой скоростью работы, но сложностью передачи самого этого закрытого ключа. Тип криптосистемы -

a. С использованием инфраструктуры открытых ключей (PKI)
b. Избыточная
c. Асиметричная
4. Симметричная

17. Предоставление полномочий на выполнение определенных действий в некоторой информационной системе называется...

a. аутентификацией
b. мандатным контролем доступа
c. авторизацией
d. инагурацией
e. идентификацией

18. При реализации механизмов безопасности при сетевом соединении, наибольшее число таких механизмов можно реализовать на следующем уровне модели OSI:

a. Физический (1)
b. Сеансовый (5)
c. Сетевой (3)
d. Транспортный (4)
e. Презентативный (6)
f. Прикладной (7)
g. Канальный (2)

19. Протокол передачи данных, обеспечивающий шифрование потока данных на транспортном уровне:

a. TCP
b. SSL
c. RDP
d. SSH
e. VPN

20. Вредоносный код обладает следующими чертами: распространяется как часть приложения, нередко имеющего привлекательный функционал (игры, программы для взлома и т.п.), что стимулирует его загрузку и запуск самим пользователем. Его тип -

a.Троянский конь
b. Червь
c. Файловый вирус
d. Макровирус

21. Доступностью в терминах информационной безопасности называется

a. возможность за приемлемое время получить требуемую информационную услугу
b. информация, изложенная доступным для понимания образом

c. актуальность и непротиворечивость информации
d. полная открытость всех информационных объектов для любых пользователей

22. Под конфиденциальностью в контексте информационной безопасности понимают
a. актуальность и непротиворечивость информации
b. защиту информации от несанкционированного доступа
c. механизм управления паролями доступа к ИС
d. степень доверия к получаемой информации

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

а) основная учебная литература:

1. Мельников, В. П. Информационная безопасность и защита информации [Текст] : учебное пособие для вузов / В. П. Мельников. - 4-е издание, стереотипное. - Москва : Академия, 2009. - 336 с. - (Высшее профессиональное образование : Информатика и вычислительная техника). - Гриф УМО "Допущено". (30 шт.)

2. Бирюков А.А. Информационная безопасность: защита и нападение. – М.: ДМК Пресс, 2012. – 474 с.: ил. ISBN 978-5-94074-647-8. Доступ: http://e.lanbook.com/books/element.php?pl1_id=39990

3. Защита информации [Электронный ресурс] : учебное пособие / А. П. Жук [и др.]. - 2-е изд. – Электрон. текстов. данные. - Москва : РИОР : ИНФРА-М, 2015. - 392 с. - (Высшее образование: Бакалавриат; Магистратура). - Режим доступа: http://znanium.com/bookread2.php?book=474838

б) дополнительная учебная литература:

1. Баранова, Е. К. Информационная безопасность и защита информации [Электронный ресурс] : учебное пособие / Е. К. Баранова , А. В. Бабаш . - 3-е изд. – Электрон. текстов. данные. - Москва : РИОР : ИНФРА-М, 2016. - 322 с. - (Высшее образование). – Режим доступа: http://znanium.com/bookread2.php?book=495249

2. Каратунова, Н. Г. Защита информации. Курс лекций [Электронный ресурс] : учебное пособие / Н. Г. Каратунова. – Электрон. текстов. данные. - Краснодар: КСЭИ, 2014. - 188 с. - Режим доступа: http://znanium.com/bookread2.php?book=503511

3. Кнауб Л. В. Теоретико-численные методы в криптографии: Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2011. - 160 с. ISBN 978-5-7638-2113-7. Доступ: http://znanium.com/catalog.php?bookinfo=441493

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Электронно-библиотечная система Издательства "Лань"» http://e.lanbook.com/ – Договор № 14-ЕП от 03.04.2017 г., срок действия - до 03.04.2018 г. Неограниченный доступ для всех зарегистрированных пользователей КемГУ и всех филиалов из любой точки доступа Интернет. Доступ из локальной сети НФИ КемГУ свободный, неограниченный, с домашних ПК – авторизованный. Кол-во возможных подключений – безлимит.

2. Электронно-библиотечная система «Знаниум» - www.znanium.com – Договор № 44/2017 от 21.02.2017 г., срок до 15.03.2020 г. Доступ из локальной сети НФИ КемГУ свободный, неограниченный, с домашних ПК – авторизованный. Кол-во возможных подключений – 4000.

3. Электронно-библиотечная система «Университетская библиотека онлайн»

http://biblioclub.ru/ – базовая часть, контракт № 031 - 01/17 от 02.02.2017 г., срок до 14.02.2018 г., неограниченный доступ для всех зарегистрированных пользователей КемГУ. Доступ из локальной сети НФИ КемГУ свободный, неограниченный, с домашних ПК – авторизованный. Кол-во возможных подключений – 7000.

4. Электронно-библиотечная система «Юрайт» - www.biblio-online.ru. Доступ ко всем произведениям, входящим в состав ЭБС. Договор № 30/2017 от 07.02.2017 г., срок до 16.02.2018г. Доступ из локальной сети НФИ КемГУ свободный, с домашних ПК – авторизованный. Кол-во одновременных доступов - безлимит .

5. Электронная полнотекстовая база данных периодических изданий по общественным и гуманитарным наукам ООО «ИВИС», https://dlib.eastview.com, договор № 196-П от 10.10.2016 г., срок действия с 01.01.2017 по 31.12.2017 г., доступ предоставляется из локальной сети НФИ КемГУ.

6. Межвузовская электронная библиотека (МЭБ) - https://icdlib.nspu.ru/ - сводный информационный ресурс электронных документов для образовательной и научно-исследовательской деятельности педагогических вузов. НФИ КемГУ является участником и пользователем МЭБ. Договор о присоединении к МЭБ от 15.10.2013 г,, доп. соглашение от 01.04.2014 г. Доступ предоставляется из локальной сети НФИ КемГУ.

7. Университетская информационная система РОССИЯ (УИС Россия) – http://uisrussia.msu.ru - база электронных ресурсов для образования и исследований в области экономики, социологии, политологии, международных отношений и других гуманитарных наук. Письмо 01/08 – 104 от 12.02.2015. Срок – бессрочно. Доступ предоставляется из локальной сети НФИ КемГУ.

9. Методические указания для обучающихся по освоению дисциплины

Вид учебных занятий	**Организация деятельности студента**
Лекция	Лекции построены на основе использования активных форм обучения: - **лекция-беседа (п**реимущество лекции-беседы состоит в том, что она позволяет привлекать внимание студентов к наиболее важным вопросам темы, определять содержание и темп изложения учебного материала с учетом особенностей студентов), - **проблемная лекция** (с помощью проблемной лекции обеспечивается достижение трех основных дидактических целей: усвоение студентами теоретических знаний; развитие теоретического мышления; формирование познавательного интереса к содержанию учебного предмета и профессиональной мотивации будущего специалиста), **--лекция с заранее запланированными ошибками** (Эта форма проведения лекции необходима для развития у студентов умений оперативно анализировать профессиональные ситуации, выступать в роли экспертов, оппонентов, рецензентов, вычленять неверную или неточную информацию). На каждой лекции применяется сочетание этих форм обучения в зависимости от подготовленности студентов и вопросов, вынесенных на лекцию. Присутствие на лекции не должно сводиться лишь к автоматической записи изложения предмета преподавателем. Более того, современный насыщенный материал каждой темы не может (по времени) совпадать с записью в тетради из-за разной скорости процессов – мышления и автоматической записи. Каждый студент должен разработать для себя систему ускоренного фиксирования на бумаге материала лекции. Поэтому, лектором ***рекомендуется формализация записи*** посредством использования общепринятых логико-математических символов, сокращений, алгебраических (формулы) и геометрических (графики), системных (схемы, таблицы) фиксаций изучаемого материала. Овладение такой методикой, позволяет каждому студенту не только ускорить процесс изучения, но и повысить его качество, поскольку успешное владение указанными приемами требует переработки,

	осмысления и структуризации материала.
Лабораторная работа	Вузовская подготовка специалистов должна обеспечивать приобретение ими не только знаний, но и умений использовать полученные знания на практике. Это требование и положено в основу целей и методов проведения лабораторных работ по вышеуказанной учебной дисциплине. Лабораторные работы предлагаются в соответствии с рабочей программой в рамках каждой темы.
Подготовка к экзамену	Подготовка к экзамену предполагает изучение рекомендуемой литературы и других источников, конспектов лекций, повторение материалов практических занятий.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Тематические презентации, антивирусное ПО, служебные программы диагностики, системы программирования, серверы учебного назначения.

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Наименование оборудованных учебных кабинетов, объектов для проведения практических занятий, объектов физической культуры и спорта (с указанием номера помещения в соответствии с документами БТИ)	**Перечень основного оборудования**	**Специализированное программное обеспечение**	**Учебно-наглядные пособия (демонстрационные материалы)**
Компьютерный класс (аудитория № 302) учебный корпус 2, Пр. Пионерский, 13, помещение № 115 по этажному *плану 3 этажа от 13.07.2004*	Увлажнитель воздуха. Персональные компьютеры с выходом в Интернет -12шт, Доска маркерная.	Windows_XP, Linux Ubuntu, Libre Office 5.0, Lazarus, Hexplorer, Wiveshark	Слайды (презентация в Microsoft Power Point)
Компьютерный класс (аудитория № 303) учебный корпус 2, Пр. Пионерский, 13, помещение № 116 по этажному *плану 3 этажа от 13.07.2004*	Персональные компьютеры с выходом в Интернет –15шт.; Доска маркерная		
Компьютерный класс (аудитория № 306) учебный корпус 2, Пр. Пионерский, 13, помещение № 121 по этажному *плану 3 этажа от 13.07.2004*	Персональные компьютеры с выходом в Интернет -12шт.		
Компьютерный класс (аудитория № 308) учебный корпус 2, Пр. Пионерский, 13, помещение № 123 по этажному *плану 3 этажа от 13.07.2004*	Персональные компьютеры с выходом в Интернет-9шт.; Доска маркерная; принтер KYOCERA		
Компьютерный класс (аудитория № 309) учебный корпус 2, Пр. Пионерский, 13, помещение № 124 по этажному *плану 3 этажа от 13.07.2004*	Персональные компьютеры с выходом в Интернет - 13шт.; Доска маркерная.		
Компьютерный класс (аудитория № 311) учебный корпус 2, Пр. Пионерский, 13, помещение № 126 по этажному *плану 3*	Персональные компьютеры с выходом в Интернет		

этажа от 13.07.2004	– 12шт		

12. Иные сведения и (или) материалы

12.1. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Для обеспечения образования инвалидов и обучающихся с ограниченными возможностями здоровья разрабатывается адаптированная образовательная программа, индивидуальный учебный план с учетом особенностей их психофизического развития и состояния здоровья.

Обучение обучающихся с ограниченными возможностями здоровья осуществляется на основе образовательных программ, адаптированных для обучения указанных обучающихся.

Обучение по образовательной программе инвалидов и обучающихся с ограниченными возможностями здоровья осуществляется факультетом с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

Университетом создаются специальные условия для получения высшего образования по образовательным программам обучающихся с ограниченными возможностями здоровья.

12.2. Перечень образовательных технологий, используемых при осуществлении образовательного процесса по дисциплине

Лекция (информационная, дискуссия, проблемная); лабораторная работа; опрос; работа со справочной системой программ; работа с информационными ресурсами; самостоятельная работа.

12.3. Занятия, проводимые в интерактивных формах

№ п/п	Раздел, тема дисциплины	Объем аудиторной работы в интерактивных формах по видам занятий (час.)		Формы работы
		лекции	лабораторные работы	
1	Многоуровневая защита корпоративных сетей.	2	2	Проблемная лекция. Работа в малых группах
2	Защита информации в сетях.	2	2	Проблемная лекция. Работа в малых группах
3	Требования к системам защиты информации.	2	4	Проблемная лекция. Работа в малых группах
	ИТОГО по дисциплине:	**6**	**8**	

Составитель (и): Читайло А.И., ст. преподаватель кафедры ТиМПИ