

Подписано электронной подписью:

Вержицкий Данил Григорьевич

Должность: Директор КГПИ ФГБОУ ВО «КемГУ»

Дата и время: 2024-02-21 00:00:00

471086fad29a3b30e244c728abc3661ab35c9d50210dcf0e75e03a5b6fdf6436

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ 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»

(Наименование филиала, где реализуется данная дисциплина)

Факультет информатики, математики и экономики
Кафедра информатики и общетехнических дисциплин

УТВЕРЖДАЮ

Декан ФИМЭ

А.В. Фомина

« 13 » февраля 2020 г.



Рабочая программа дисциплины
Б1.В.ДВ.14.01 Методы и средства защиты информации

Направление подготовки

44.03.05 Педагогическое образование (с двумя профилями подготовки)

Направленность (профиль) подготовки

Информатика и Физика

Программа *академического бакалавриата*

Квалификация выпускника

бакалавр

Форма обучения

Очная

Год набора 2016

Новокузнецк 2020

Лист внесения изменений

в РПД Б1.В.ДВ.14.01 Методы и средства защиты информации

Сведения об утверждении:

утверждена Ученым советом факультета информатики, математики и экономики
(протокол Ученого совета факультета № 9 от 14.02.2019)

для ОПОП 2016 год набора _____ на 2019 / 2020 учебный год
по направлению подготовки 44.03.05 Педагогическое образование _____
(код и название направления подготовки / специальности)

направленность (профиль) подготовки Информатика и Физика

Одобрена на заседании методической комиссии факультета
протокол методической комиссии факультета № 6 от 14.02.2019)

Одобрена на заседании обеспечивающей кафедры ИОТД
протокол № 5 от 19.01.2019г. Можаров М.С / _____
(Ф. И.О. зав. кафедрой) (Подпись)

Переутверждение на учебный год:

на 2020 / 2021 учебный год

утверждена Ученым советом факультета _____
(протокол Ученого совета факультета № 8 от 13.02.20 г.

Одобрена на заседании методической комиссии факультета _____
протокол методической комиссии факультета № 6 от 06.02.2020г.

Одобрена на заседании обеспечивающей кафедры _____
протокол № 5 от 19.12.2019 г. Можаров М.С / _____
(Ф. И.О. зав. кафедрой) (Подпись)

на 20 ____ / 20 ____ учебный год

утверждена _____ Ученым _____ советом _____ факультета
(протокол Ученого совета факультета № ____ от 201 ____ г.

Одобрена на заседании методической комиссии факультета _____
протокол методической комиссии факультета № ____ от 20 ____ г.

Одобрена на заседании обеспечивающей кафедры _____
протокол № ____ от ____ . ____ . 20 ____ г. _____ / _____
(Ф. И.О. зав. кафедрой) (Подпись)

на 20 ____ / 20 ____ учебный год

утверждена _____ Ученым _____ советом _____ факультета
(протокол Ученого совета факультета № ____ от 201 ____ г.

Одобрена на заседании методической комиссии факультета _____
протокол методической комиссии факультета № ____ от 20 ____ г.

Одобрена на заседании обеспечивающей кафедры _____
протокол № ____ от ____ . ____ . 20 ____ г. _____ / _____
(Ф. И.О. зав. кафедрой) (Подпись)

Оглавление

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения основной образовательной программы «Педагогическое образование» по профилю "Информатика и физика"	4
2. Место дисциплины в структуре ООП бакалавриата	4
3. Объем дисциплины (модуля) 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 (модуля) по видам учебных занятий (в часах)	4
4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий	5
4.1. Разделы дисциплины (модуля) и трудоемкость по видам учебных занятий (в академических часах)	5
4.2. Содержание дисциплины (модуля), структурированное по темам (разделам)	6
5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)	8
6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)	8
6.1. Типовые контрольные задания или иные материалы	8
6.2. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций	12
7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)	13
а) основная учебная литература	13
б) дополнительная учебная литература	13
8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)	13
9. Методические указания для обучающихся по освоению дисциплины (модуля)	13
10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)	14

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения основной образовательной программы «Педагогическое образование» по профилю "Информатика и физика"

В результате освоения ООП бакалавриата обучающийся должен овладеть следующими результатами обучения по дисциплине (модулю):

Коды компетенции	Результаты освоения ООП Содержание компетенций	Перечень планируемых результатов обучения по дисциплине
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 с нормативно-правовыми документами сферы образования; нормативными документами по вопросам обучения и воспитания детей и молодежи.

2. Место дисциплины в структуре ООП бакалавриата

Дисциплина «Методы и средства защиты информации» относится к вариативной части профессионального цикла дисциплин.

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 (модуль) изучается на __5__ курсе (ах) в __10__ семестре.

3. Объем дисциплины (модуля) 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 (модуля) составляет __4__ зачетных единиц (ЗЕТ), __144__ академических часа.

3.1. Объем дисциплины (модуля) по видам учебных занятий (в часах)

Объем дисциплины	Всего часов
------------------	-------------

	для очной формы обучения	для заочной /очно-заочной формы обучения
Общая трудоемкость дисциплины	144	
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	44	
Аудиторная работа (всего**):	36	
в т. числе:		
Лекции	14	
Семинары, практические занятия		
Практикумы		
Лабораторные работы	30	
Занятия в интерактивной форме	10	
Внеаудиторная работа (всего**):	64	
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)	64	
Вид промежуточной аттестации обучающегося (зачет / экзамен)	Экзамен, 36	

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

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

для очной формы обучения

№ п/п	Раздел дисциплины	Общая трудоем кость (часах)	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах)			Формы текущего контроля успеваемост и
			аудиторные учебные занятия		самостоя- тельная работа обучаю- щихся	
		всего	лекции	семинары, практи- ческие занятия		
1.	Основные понятия информационной безопасности систем. Источники атак на информацию, риски.	8	2	2	4	Устный опрос, лабораторная работа
2.	Политика безопасности. Стандарты безопасности.	8	2	2	4	Устный опрос, лабораторная работа

№ п/п	Раздел дисциплины	Общая трудоем- кость (часах)	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах)			Формы текущего контроля успеваемости и
			аудиторные учебные занятия		самостоя- тельная работа обучаю- щихся	
		всего	лекции	семинары, практи- ческие занятия		
3.	Криптографические модели. Алгоритмы шифрования.	10	2	2	6	Тест, лаборатор- ная работа
4.	Модели безопасности основных ОС.	8	2	2	4	Тест, лаборатор- ная работа
5.	Алгоритмы аутентификации пользователей.	8	2	2	4	Тест, лаборатор- ная работа
6.	Многоуровневая защита корпоративных сетей.	12	4	4	4	Тест, лаборатор- ная работа
7.	Защита информации в сетях.	10	2	2	6	Тест, лаборатор- ная работа
8.	Требования к системам защиты информации.	8	2	2	4	Тест, лаборатор- ная работа

4.2 Содержание дисциплины (модуля), структурированное по темам (разделам)

№ п/п	Наименование раздела дисциплины	Содержание
<i>Содержание лекционного курса</i>		
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

№ п/п	Наименование раздела дисциплины	Содержание
		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).
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.	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.
8	Требования к системам защиты информации.	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.
<i>Темы лабораторных занятий</i>		
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 (модулю)

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.

Методические указания по самостоятельной работе размещены по адресу:

<https://skado.dissw.ru/table>

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

6.1. Типовые контрольные задания или иные материалы

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 информации о состоянии сети

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

- a. Избыточная
- b. Симметричная
- c. Асимметричная
- 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. сбой 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. Асимметричная
- d. Симметричная

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

- a. аутентификацией
- b. мандатным контролем доступа
- c. авторизацией
- d. инаугурацией
- 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
- актуальность и непротиворечивость информации
 - защиту информации от несанкционированного доступа
 - механизм управления паролями доступа к ИС
 - степень доверия к получаемой информации

6.2. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Промежуточная аттестация по дисциплине зачет включает следующие формы контроля: тестирование.

С целью определения уровня овладения компетенциями, закрепленными за дисциплиной, в заданные преподавателем сроки проводится текущий и промежуточный контроль знаний, умений и навыков каждого обучающегося. Все виды текущего контроля осуществляются на практических занятиях. При оценке компетенций принимается во внимание формирование профессионального мировоззрения, определенного уровня культуры, этические навыки, навыки владения вычислительной техникой и программными продуктами для решения практических задач. Процедура оценивания компетенций обучающихся основана на следующих стандартах:

- Периодичность проведения оценки (1 раз в неделю).
- Многоступенчатость: оценка (как преподавателем, так и студентами группы) и самооценка обучающегося, обсуждение результатов и комплекс мер по устранению недостатков.
- Единство используемой технологии для всех обучающихся, выполнение условий сопоставимости результатов оценивания.

Балльно-рейтинговая оценка результатов учебной работы обучающихся по видам (БРС)

Составляющие учебной работы	Сумма баллов	Учебная деятельность студента	Оценка в аттестации	Баллы
Текущая учебная работа в семестре	80	Посещение занятий по расписанию.	1-2 балл посещение 1 занятия	9 - 18
		Лабораторные работы	2 балла - посещение 1 практического или лабораторного занятия и выполнение работы на 51-65% 3 балла - посещение 1 практического или лабораторного занятия и выполнение работы на 66-85% 4 балла – посещение 1 занятия и существенный вклад на занятии в работу всей группы, самостоятельность и выполнение работы на 86-100%	18 - 36
		Контрольная работа	24 балла (пороговое значение) 46 баллов (максимальное значение)	24-46
Итого по текущей работе в семестре				51 - 100
Промежуточная аттестация (зачет)	20 (100 баллов приведенной шкалы)	Тест.	3 балла (пороговое значение) 10 баллов (максимальное значение)	3 - 10
		Практическая часть	7 баллов (пороговое значение) 10 баллов (максимальное значение)	7 - 10
Итого по промежуточной аттестации (зачету)				(51 – 100% по приведенной шкале)

	10 – 20 б.
Суммарная оценка по дисциплине/ Сумма баллов по текущей и промежуточной аттестации	51 – 100
б.	

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

а) основная учебная литература:

1. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] : учебное пособие / В. Ф. Шаньгин. – Электрон. текстов. данные. – Москва : ДМК, 2010. – 544 с. – (Администрирование и защита). – Режим доступа: <http://e.lanbook.com/book/1122>
2. Щербаков, А. Современная компьютерная безопасность. Теоретические основы. Практические аспекты [Электронный ресурс] : учебное пособие / А. Щербаков. – Электрон. текстов. данные. – Москва : Книжный мир, 2009. – 352 с. – (Высшая школа). – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=89798>

б) дополнительная учебная литература:

1. Бабаш А.В. Криптографические методы защиты информации. Том 3: Учебно-методическое пособие. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 216 с. ISBN 978-5-369-01304-5. Доступ: <http://znanium.com/catalog.php?bookinfo=432654>
2. Баранова Е.К., Бабаш А.В. Моделирование системы защиты информации: Практикум: Учебное пособие. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015 - 120 с. ISBN 978-5-369-01379-3. Доступ: <http://znanium.com/catalog.php?bookinfo=476047>
3. Гвоздева В.А., Лаврентьева И.Ю. Основы построения автоматизированных информационных систем: Учебник. - М.: ИД ФОРУМ: НИЦ Инфра-М, 2013. - 320 с.: ил. ISBN 978-5-8199-0315-5. Доступ: <http://znanium.com/catalog.php?bookinfo=392285>
4. 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>
5. Корпоративные информационные системы управления: Учебник / Под науч. ред. Н.М. Абдикеева, О.В. Китовой. - М.: ИНФРА-М, 2011. - 464 с. ISBN 978-5-16-004373-9. Доступ: <http://znanium.com/catalog.php?bookinfo=200718>
6. Партыка Т.Л., Попов И.И. Информационная безопасность: Учебное пособие. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с.: ил. ISBN 978-5-91134-627-0. Доступ: <http://znanium.com/catalog.php?bookinfo=420047>

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

1. Национальный открытый университет Интуит. –режим доступа <http://www.intuit.ru/>
2. Новая электронная библиотека – www.newlibrary.ru
3. Российское образование (федеральный портал) – www.edu.ru
4. ЭБС “Знаниум» - www.znanium.com
5. Универсальная справочная база данных – www.ivis.ru

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Вид учебных занятий	Организация деятельности студента
---------------------	-----------------------------------

Лекция	Лекции построены на основе использования активных форм обучения: - лекция-беседа (преимущество 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.

Методические указания размещены на сайте *НФИ КемГУ*
<https://eios.nbikemsu.ru/>

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Материально-техническая база

Учебные занятия по дисциплине проводятся в учебных аудиториях НФИ КемГУ:

Методы и средства защиты информации	303 Компьютерный класс. Учебная аудитория (мультимедийная) для проведения занятий: - лабораторного (практического) типа; - групповых и индивидуальных	654027, Кемеровская область - Кузбасс, г. Новокузнецк, пр-кт Пионерский, д.13, пом. 2
-------------------------------------	--	---

	консультаций; - текущего контроля и промежуточной аттестации. Специализированная (учебная) мебель: доска маркерно-меловая, столы компьютерные, стулья. Оборудование для презентации учебного материала: <i>стационарное</i> - ноутбук преподавателя, экран, проектор. Оборудование: компьютеры для обучающихся (11 шт.). Используемое программное обеспечение: MSWindows (MicrosoftImaginePremium 3 year по лицензионному договору № 1212/KMP от 12.12.2018 г. до 12.12.2021 г.), LibreOffice (свободно распространяемое ПО), BloodshedDevC++ 4.9.9.2 (свободно распространяемое ПО), FoxitReader (свободно распространяемое ПО), Firefox 14 (свободно распространяемое ПО), Java (бесплатная версия), MicrosoftSQLServer 2008 (MicrosoftImaginePremium 3 year по лицензионному договору № 1212/KMP от 12.12.2018 г. до 12.12.2021 г.), AdobeReaderXI(свободно распространяемое ПО), WinDjView(свободно распространяемое ПО), Интернет с обеспечением доступа в ЭИОС.	
--	--	--

Составитель (и): Читайло А.И., ст. преподаватель
(фамилия, инициалы и должность преподавателя (ей))

Макет рабочей программы дисциплины (модуля) разработан в соответствии с приказом Минобрнауки России от 19.12.2013 № 1367, одобрен научно-методическим советом (протокол № 8 от 09.04.2014 г.) и утвержден приказом ректора от 23.04.2014 № 224/10..

Макет обновлён с поправками в части подписей на титульной странице, п.3 добавлена строка для указания часов, проводимых в активной и интерактивной формах обучения, добавлен п. 12.1 Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья (протокол НМС № 6 от 15.04.2015 г.), утвержден приказом ректора.