

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное учреждение
высшего профессионального образования
"Казанский (Приволжский) федеральный университет"
Инженерный институт



подписано электронно-цифровой подписью

Программа дисциплины

Основы информационной безопасности Б2.ДВ.4

Направление подготовки: 221400.62 - Управление качеством

Профиль подготовки: не предусмотрено

Квалификация выпускника: бакалавр

Форма обучения: очное

Язык обучения: русский

Автор(ы):

Агачев Ю.Р.

Рецензент(ы):

Галимянов А.Ф.

СОГЛАСОВАНО:

Заведующий(ая) кафедрой: Авхадиев Ф. Г.

Протокол заседания кафедры No ____ от " ____ " _____ 201__ г

Учебно-методическая комиссия Инженерного института:

Протокол заседания УМК No ____ от " ____ " _____ 201__ г

Регистрационный No 868114714

Казань

2014

Содержание

1. Цели освоения дисциплины
2. Место дисциплины в структуре основной образовательной программы
3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля
4. Структура и содержание дисциплины/ модуля
5. Образовательные технологии, включая интерактивные формы обучения
6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов
7. Литература
8. Интернет-ресурсы
9. Материально-техническое обеспечение дисциплины/модуля согласно утвержденному учебному плану

Программу дисциплины разработал(а)(и) доцент, к.н. (доцент) Агачев Ю.Р. Кафедра теории функций и приближений отделение математики, Juriy.Agachev@kpfu.ru

1. Цели освоения дисциплины

Целями освоения дисциплины БЗ.Б.9. "Основы информационной безопасности" являются знакомство с понятиями национальной безопасности; видами безопасности; информационной безопасности (ИБ) в системе национальной безопасности Российской Федерации; основными понятиями, общеметодологическими принципами теории ИБ; анализом угроз ИБ, проблемами информационной войны; государственной информационной политикой; проблемами региональной информационной безопасности; видами информации; методами и средствами обеспечения ИБ; методами нарушения конфиденциальности, целостности и доступности информации; причинами, видами, каналами утечки и искажения информации.

2. Место дисциплины в структуре основной образовательной программы высшего профессионального образования

Данная учебная дисциплина включена в раздел " Б2.ДВ.4 Общепрофессиональный" основной образовательной программы 221400.62 Управление качеством и относится к дисциплинам по выбору. Осваивается на 1 курсе, 2 семестр.

Изучение данной дисциплины базируется на подготовке по физике, математике и информатике

3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОК-11 (общекультурные компетенции)	способность понимать сущность и значение информации в развитии современного информационного общества сознавать опасность и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны
ОК-12 (общекультурные компетенции)	владеть основными методами, способами и средствами получения, хранения, переработки информации, иметь навыки работы с компьютером как средством управления информацией
ОК-13) (общекультурные компетенции)	способностью работать с компьютером как средством управления информацией (ОК-13);
ОК-14 (общекультурные компетенции)	способностью работать с информацией в глобальных компьютерных сетях (ОК-14);
ОК-18 (общекультурные компетенции)	способностью понимать сущность и значение информации в развитии современного информационного общества, осознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны (

В результате освоения дисциплины студент:

1. должен знать:

Терминологию в области информационной безопасности, методы и средства обеспечения информационной безопасности, методы нарушения конфиденциальности, целостности и доступности информации. Содержание основных понятий по правовому обеспечению информационной безопасности; основы безопасности операционных систем; основы безопасности вычислительных сетей; основные технические средства и методы защиты информации; основные программно-аппаратные средства обеспечения информационной безопасности.

2. должен уметь:

Правильно проводить анализ угроз информационной безопасности, выполнять основные этапы решения задач информационной безопасности, применять на практике основные общеметодологические принципы теории информационной безопасности.

Отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации; применять действующую законодательную базу в области информационной безопасности; разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов.

3. должен владеть:

- выполнять полный объем работ, связанных с комплексным обеспечением информационной безопасности конкретных автоматизированных систем на основе разработанных программ и методик, в том числе с обеспечением требований нормативных документов, регламентирующих режим соблюдения государственной тайны;

- к анализу материалов организаций и подразделений ведомства с целью подготовки принятия решений по обеспечению защиты информации;

- выполнять оперативное управление деятельностью организаций по комплексному обеспечению информационной безопасности конкретных автоматизированных систем на основе разработанных программ и методик.

4. должен демонстрировать способность и готовность:

- выполнять полный объем работ, связанных с комплексным обеспечением информационной безопасности конкретных автоматизированных систем на основе разработанных программ и методик, в том числе с обеспечением требований нормативных документов, регламентирующих режим соблюдения государственной тайны;

- к анализу материалов организаций и подразделений ведомства с целью подготовки принятия решений по обеспечению защиты информации;

- выполнять оперативное управление деятельностью организаций по комплексному обеспечению информационной безопасности конкретных автоматизированных систем на основе разработанных программ и методик.

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 2 зачетных(ые) единиц(ы) 72 часа(ов).

Форма промежуточного контроля дисциплины зачет во 2 семестре.

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

55-70 баллов - "удовлетворительно" (удов.);

54 балла и менее - "неудовлетворительно" (неуд.).

4.1 Структура и содержание аудиторной работы по дисциплине/ модулю Тематический план дисциплины/модуля

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Информационная безопасность в системе национальной безопасности РФ: Понятие национальной безопасности. Виды безопасности: экономическая внутриполитическая, социальная, военная. международная, информационная, экологическая и другие. Соотношение безопасности личности, общества и государства. Виды защищаемой информации. Роль информационной безопасности в обеспечение нацио-нальной безопасности государства.	2	1-2	6	0	0	устный опрос
2.	Тема 2. Основы государственной политики РФ в обла-сти нформационной безопасности (ИБ): Национальные интересы РФ в информационной сфере и их обеспечение. Виды угроз национальной безопасности РФ. Источники угроз ИБ РФ	2	3-6	8	0	0	устный опрос

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
3.	Тема 3. Информационная война, методы и средства её ведения: Информационная безопасность и информационное противоборство. Информационное оружие, его классификация и возможности. Методы нарушения конфиденциальности, целостности и доступности информации. Причины, виды, каналы утечки и искажения информации. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны	2	7-11	10	0	0	устный опрос

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
4.	Тема 4. Методы и средства обеспечения ИБ объектов информа-ционной сферы. Правовые, организационно-технические и экономические методы обеспечения я ИБ. Модели, стратегии и системы обеспечения ИБ. Критерии и классы защищенности средств вычислительной техники и автоматизи-рованных информа-ционных систем. Методы и средства обеспече-ния ИБ компьютерных систем.	2	12-17	12	0	0	устный опрос
	Тема . Итоговая форма контроля	2		0	0	0	зачет
	Итого			36	0	0	

4.2 Содержание дисциплины

Тема 1. Информационная безопасность в системе национальной безопасности РФ:

Понятие национальной безопасности. Виды безопасности: экономическая внутриполитическая, социальная, военная. международная, информационная, экологическая и другие. Соотношение безопасности личности, общества и государства. Виды защищаемой информации. Роль информационной безопасности в обеспечение нацио-нальной безопасности государства.

лекционное занятие (6 часа(ов)):

Информационная безопасность в системе национальной безопасности РФ: Понятие национальной безопасности. Виды безопасности: экономическая внутриполитическая, социальная, военная. международная, информационная, экологическая и другие. Соотношение безопасности личности, общества и государства. Виды защищаемой информации. Роль информационной безопасности в обеспечение нацио-нальной безопасности государства.

Тема 2. Основы государственной политики РФ в обла-сти нформационной безопасности (ИБ): Национальные интересы РФ в информационной сфере и их обеспечение. Виды угроз национальной безопасности РФ. Источники угроз ИБ РФ

лекционное занятие (8 часа(ов)):

Основы государственной политики РФ в обла-сти нформационной безопасности (ИБ): Национальные интересы РФ в информационной сфере и их обеспечение. Виды угроз национальной безопасности РФ. Источники угроз ИБ РФ

Тема 3. Информационная война, методы и средства её ведения: Информационная безопасность и информационное противоборство. Информационное оружие, его классификация и возможности. Методы нарушения конфиденциальности, целостности и доступности информации. Причины, виды, каналы утечки и искажения информации. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны
лекционное занятие (10 часа(ов)):

Информационная война, методы и средства её ведения: Информационная безопасность и информационное противоборство. Информационное оружие, его классификация и возможности. Методы нарушения конфиденциальности, целостности и доступности информации. Причины, виды, каналы утечки и искажения информации. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны

Тема 4. Методы и средства обеспечения ИБ объектов информационной сферы. Правовые, организационно-технические и экономические методы обеспечения ИБ. Модели, стратегии и системы обеспечения ИБ. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Методы и средства обеспечения ИБ компьютерных систем.
лекционное занятие (12 часа(ов)):

Методы и средства обеспечения ИБ объектов информационной сферы. Правовые, организационно-технические и экономические методы обеспечения ИБ. Модели, стратегии и системы обеспечения ИБ. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Методы и средства обеспечения ИБ компьютерных систем.

4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
1.	Тема 1. Информационная безопасность в системе национальной безопасности РФ: Понятие национальной безопасности. Виды безопасности: экономическая, внутривнутриполитическая, социальная, военная, международная, информационная, экологическая и другие. Соотношение безопасности личности, общества и государства. Виды защищаемой информации. Роль информационной безопасности в обеспечении национальной безопасности					

государства.

2

1-2

подготовка к
устному опросу

6

устный опрос

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
2.	Тема 2. Основы государственной политики РФ в области информационной безопасности (ИБ): Национальные интересы РФ в информационной сфере и их обеспечение. Виды угроз национальной безопасности РФ. Источники угроз ИБ РФ	2	3-6	подготовка к устному опросу	8	устный опрос
3.	Тема 3. Информационная война, методы и средства её ведения: Информационная безопасность и информационное противоборство. Информационное оружие, его классификация и возможности. Методы нарушения конфиденциальности, целостности и доступности информации. Причины, виды, каналы утечки и искажения информации. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны	2	7-11	подготовка к устному опросу	10	устный опрос

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
4.	Тема 4. Методы и средства обеспечения ИБ объектов информационной сферы. Правовые, организационно-технические и экономические методы обеспечения ИБ. Модели, стратегии и системы обеспечения ИБ. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Методы и средства обеспечения ИБ компьютерных систем.	2	12-17	подготовка к устному опросу	12	устный опрос
	Итого				36	

5. Образовательные технологии, включая интерактивные формы обучения

Используются следующие формы учебной работы: лекции, практические занятия, самостоятельная работа студента (выполнение индивидуальных домашних заданий), консультации. Материалы курса лекций, список контрольных вопросов, задания для практических занятий и самостоятельной работы имеются в электронном варианте.

Консультации проводятся в обозначенное в расписании время и в режиме "online".

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

Тема 1. Информационная безопасность в системе национальной безопасности РФ: Понятие национальной безопасности. Виды безопасности: экономическая, внутриполитическая, социальная, военная, международная, информационная, экологическая и другие. Соотношение безопасности личности, общества и государства. Виды защищаемой информации. Роль информационной безопасности в обеспечении национальной безопасности государства.

устный опрос, примерные вопросы:

Устный опрос по дисциплине проводится в форме проблемно-исследовательской беседы, в ходе которой обсуждаются следующие вопросы: Информационная безопасность в системе национальной безопасности РФ: Понятие национальной безопасности. Виды безопасности: экономическая, внутриполитическая, социальная, военная, международная, информационная, экологическая и другие. Соотношение безопасности личности, общества и государства. Виды защищаемой информации. Роль информационной безопасности в обеспечении национальной безопасности государства.

Тема 2. Основы государственной политики РФ в области информационной безопасности (ИБ): Национальные интересы РФ в информационной сфере и их обеспечение. Виды угроз национальной безопасности РФ. Источники угроз ИБ РФ

устный опрос, примерные вопросы:

Устный опрос по дисциплине проводится в форме проблемно-исследовательской беседы, в ходе которой обсуждаются следующие вопросы: Основы государственной политики РФ в области информационной безопасности (ИБ): Национальные интересы РФ в информационной сфере и их обеспечение. Виды угроз национальной безопасности РФ. Источники угроз ИБ РФ

Тема 3. Информационная война, методы и средства её ведения: Информационная безопасность и информационное противоборство. Информационное оружие, его классификация и возможности. Методы нарушения конфиденциальности, целостности и доступности информации. Причины, виды, каналы утечки и искажения информации. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны

устный опрос, примерные вопросы:

Устный опрос по дисциплине проводится в форме проблемно-исследовательской беседы, в ходе которой обсуждаются следующие вопросы: Информационная война, методы и средства её ведения: Информационная безопасность и информационное противоборство. Информационное оружие, его классификация и возможности. Методы нарушения конфиденциальности, целостности и доступности информации. Причины, виды, каналы утечки и искажения информации. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны

Тема 4. Методы и средства обеспечения ИБ объектов информационной сферы. Правовые, организационно-технические и экономические методы обеспечения ИБ. Модели, стратегии и системы обеспечения ИБ. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Методы и средства обеспечения ИБ компьютерных систем.

устный опрос, примерные вопросы:

Устный опрос по дисциплине проводится в форме проблемно-исследовательской беседы, в ходе которой обсуждаются следующие вопросы: Методы и средства обеспечения ИБ объектов информационной сферы. Правовые, организационно-технические и экономические методы обеспечения ИБ. Модели, стратегии и системы обеспечения ИБ. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Методы и средства обеспечения ИБ компьютерных систем.

Тема . Итоговая форма контроля

Примерные вопросы к зачету:

Итоговый контроль осуществляется в форме устного экзамена, на котором студентам необходимо ответить на вопросы экзаменационных билетов. Результат итогового контроля проставляется в приложении к диплому.

На экзамене студент имеет возможность получить максимальное число баллов - 50. Студент может получить следующие оценки с учетом продемонстрированных знаний:

- 41-50 баллов - студент должен безошибочно ответить на вопросы, представленные в билете, а также продемонстрировать свободное владение материалом при ответе на дополнительные вопросы;
- 31-40 баллов - студент безошибочно ответил на вопросы, представленные в билете, но не точно или не в полном объеме раскрыл дополнительно заданные вопросы;
- 21-30 баллов - студент ответил на вопросы, представленные в билете, но затрудняется в ответах на дополнительные вопросы;
- 11-20 баллов - студент затрудняется в ответах на вопросы билета, отвечает только после наводящих вопросов, демонстрируя слабое знание при ответе на дополнительные вопросы;
- 10 баллов и менее - студент продемонстрировал слабые знания при ответе на вопросы, сформулированные в билете, не ответил ни на один из дополнительных вопросов;
- 0 баллов - студент не ответил ни на один из вопросов билета. После подготовки по второму (дополнительному) билету также не продемонстрировал знаний по данному предмету. Студент, не явившийся на экзамен без уважительной причины, также получает 0 баллов.

Перечень вопросов к экзамену:

1. Основная идея теории информации по К. Шеннону, её отличие от семантической теории информации по Ю.А. Шрейдеру.
2. Виды информации, её свойства и особенности их взаимодействия.
3. Соотношение между материей и информацией.
4. Понятие информации по К. Шеннону и Н. Винеру.
5. Семантический, лингвистический, прагматический и технический аспекты информации.
6. Основные признаки информации.
7. Информация, данные и знание, их взаимосвязь и различие.
8. Основные документы, определяющие концептуальные основы информационной безопасности РФ.
9. Концепция национальной безопасности РФ. Важнейшие задачи обеспечения национальной безопасности в информационной сфере.
10. Доктрина информационной безопасности.
11. Понятие национальных интересов.
12. Национальные интересы страны в информационной сфере, угрозы национальным интересам.

13. Причины и источники угроз национальным интересам страны.
14. Виды безопасности.
15. Национальная безопасность и её составляющие.
16. Субъекты системы и уровни обеспечения национальной безопасности РФ.
17. Основные задачи по обеспечению национальной безопасности.
18. Возможные сценарии подрыва безопасности России без применения военных средств.
19. Понятие "Информационной безопасности".
20. Место информационной безопасности в системе национальной безопасности России.
21. Важнейшие федеральные нормативные правовые акты, касающиеся информационной безопасности.
22. Законы, непосредственно касающиеся защиты компьютерной информации.
23. Информация и право. Информация как объект правового регулирования.
24. Информационные отношения.
25. Законы, действующие в области производства, распространения и потребления информации.
26. Информационная война, методы и средства её ведения.
27. Информационное оружие, его классификация и возможности.
28. Методы нарушения конфиденциальности, целостности и доступности информации.
29. Причины, виды, каналы утечки и искажения информации.
30. Основные направления обеспечения информационной безопасности объектов информационной сферы.
31. Методы и средства обеспечения ИБ объектов информационной сферы.
32. Стандарты и нормативы в сфере обеспечения информационной безопасности.
33. Определение безопасности компьютерной системы и категории требований безопасности.

34. Базовые требования безопасности компьютерной системы.
35. Классы безопасности компьютерных систем, понятие риска.
36. Сущность понятий: "Вычислительная база защиты", "Монитор обращений", "Ядро безопасности".
37. Режимы функционирования компьютерной системы.
38. Сущность понятий: идентификация, аутентификация; авторизация.
39. Адекватность средств защиты.
40. Понятие продукта ИТ и системы обработки информации.
39. Классы средств защиты информации.
40. Федеральная целевая программа "Электронная Россия".

7.1. Основная литература:

1. Бабаш А В Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2 <http://znanium.com/bookread.php?book=405000>
2. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с.: ил.; 60x90 1/16. - (Профессиональное образование). (переплет) ISBN 978-5-8199-0331-5, 1000 экз.<http://znanium.com/bookread.php?book=423927>
3. Данилова Е А., Золотарев, В. В. Управление информационной безопасностью. Ч. 1. Анализ информационных рисков [Электронный ресурс] : учеб. пособие/ В. В. Золотарев, Е. А. Данилова. - Красноярск :Сиб. гос. аэрокосмич. ун-т, 2010. - 144 с.<http://znanium.com/bookread.php?book=463037>

4. Золотарев В В., Жукова, М. Н. Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности [Электронный ресурс] : учеб. пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 100 с.<http://znanium.com/bookread.php?book=463061>

7.2. Дополнительная литература:

Информационная война. Проблемы и модели, Расторгуев, Сергей Павлович, 2006г.

1. Хорев П. Б. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. - М.: Форум, 2009. - 352 с.: ил.; 60x90 1/16. - (Высшее образование). (переплет) ISBN 978-5-91134-353-8, 1500 экз.<http://znanium.com/bookread.php?book=169345>

2. Дубинин Е. А. Оценка относительного ущерба безопасности информационной системы: Монография / Е.А. Дубинин, Ф.Б. Тебуева, В.В. Копытов. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 192 с.: ил.; 60x88 1/16 + 11 с.. - (Научная мысль). (о) ISBN 978-5-369-01371-7, 500 экз. <http://znanium.com/bookread.php?book=471787>

7.3. Интернет-ресурсы:

Web-сервер подразделения по выявлению и пресечению преступлений, совершаемых с использованием поддельных кредитных карт, и преступлений, совершаемых путем несанкционированного доступа в компьютерные сети и базы данных - <http://www.cyberpolice.ru>

Информационный бюллетень "Jet Info" с тематическим разделом по информационной безопасности - <http://www.jetinfo.ru/>

портал по информационной безопасности - <http://www.infosecurity.report.ru/>

портал по информационной безопасности - <http://www.void.ru/>

Сервер компании НИП "Информзащита" - <http://www.infosec.ru/>

Украинский Центр информационной безопасности - <http://www.bezpeka.com/>

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Основы информационной безопасности" предполагает использование следующего материально-технического обеспечения:

В процессе освоения дисциплины используются следующие образовательные технологии, способы и методы формирования компетенций: лекции с просмотром видео- и мультимедийных материалов (презентации ppt) и устный опрос в форме проблемно-исследовательской беседы.

Для проведения таких занятий необходима мультимедийная аудитория.

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 221400.62 "Управление качеством" и профилю подготовки не предусмотрено .

Автор(ы):

Агачев Ю.Р. _____

"__" _____ 201__ г.

Рецензент(ы):

Галимянов А.Ф. _____

"__" _____ 201__ г.