РАБОЧАЯ ПРОГРАММА

Дисциплина:	«Обеспечение информационной безопасности»
Наименование кафедры (ПЦК, отделения и др.)	Экономики и организации производства (ЭиОП)

Направление 38.04.01 – «Экономика» (степень - магистр)
Профиль: «Экономическая безопасность организации»

Сведения о разработчиках:

ФИО	Аббревиатура кафедры (ПЦК, отделения и др.)	Ученая степень, звание
Барашков С.В.	ЭиОП	к.э.н., доцент

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Рабочая программа учебной дисциплины « предназначена для реализации государственных требований к содержанию и уровню подготовки магистров по направлениям высшего профессионального образования «Экономическая безопасность»

Цель освоения дисциплины: формирование у студентов целостного понимания организации и управления информационными процессами в организации и обеспечения на этой основе качественной подготовки в области информационно-управляющих и информационно-коммуникационных методов и средств, используемых в организации при решении задач различного назначения и содержания.

Задачами, которые должны быть решены в процессе реализации данной учебной программы, являются:

- освоение типовых информационных процессов, реализуемых в организации при решении различных управленческих задач;

- определение основных угроз информационной безопасности, возникающих в процессе функционирования организации;

- освоение типовых методов и средств предотвращения и ликвидации ущерба, который может быть нанесен организации при реализации различных угроз информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП:

Рабочая программа учебной дисциплины «Компьютерные технологии и информационная безопасность» предназначена для реализации государственных требований к содержанию и уровню подготовки выпускников по направлению высшего профессионального образования «Экономика» (профиль «Экономическая безопасность организации») и является единой для всех форм обучения.

Учебная дисциплина «Компьютерные технологии и информационная безопасность» направлена на формирование у слушателей целостного понимания организации и управления информационными процессами в организации и обеспечения на этой основе качественной подготовки в области информационно-управляющих и информационно-коммуникационных методов и средств, используемых в организации при решении задач различного назначения и содержания.

Освоение данного курса основано на компетенциях бакалавров и специалистов, сформированных в процессе изучения следующих дисциплин:

Информатика;

Информационные системы в экономике;

Информационные технологии в экономике;

Информационные технологии в менеджменте;

Менеджмент.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций:

готовность действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения (ОК-2);

способностью принимать организационно-управленческие решения (ОПК-3);

способностью готовить аналитические материалы для оценки мероприятий в области экономической политики и принятия стратегических решений на микро- и макроуровне (ПК-8);

способность анализировать и использовать различные источники информации для проведения экономических расчетов (ПК-9).

В результате изучения дисциплины студент должен:

Знать:

основные положения нормативно-методических документов различного уровня в области информационной безопасности.

Уметь:

готовить задания и разрабатывать проектные решения с учетом фактора неопределенности и необходимости обеспечивать информационную безопасность организации;

готовить задания и разрабатывать методические и нормативные документы, а также предложений и мероприятий по реализации разработанных проектов и программ в области внедрения методов и средств обработки информации и обеспечения информационной безопасности;

анализировать существующие формы организации управления; разрабатывать и обосновывать предложения по их совершенствованию с учетом информационных рисков и средств их минимизации.

Владеть:

основными методами и средствами обработки информации в процессе подготовки и реализации управленческих решений в организации.

В результате освоения данного курса у слушателя должна быть сформирована парадигма рационального управления организацией как совокупностью технологических процессов обработки информации. С учетом ценности информации различного содержания, которая циркулирует по каналам связи в организации и пересылается партнерам организации по экономической деятельности во внешней среде, критерием рациональности

задач управления, так или иначе рассматриваемых в рамках курса, является минимизация информационных рисков, имеющих место в организации.

4. ОБЩАЯ ТРУДОЁМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (4)

4.2. Объем дисциплины и виды учебной работы (144):

Вид учебной работы	Количество часов (форма обучения очная)	
	Всего по плану	В том числе по семестрам
		№ семестра 2
Контактная работа обучающихся с преподавателем	48	48
Аудиторные занятия:	48	48
Лекции	16	16
Практические и семинарские занятия	32	32
Самостоятельная работа	60	60
Промежуточный контроль - экзамен	36	36
Всего часов по дисциплине	144	144

4.3.Распределение часов по темам и видам учебной работы:

Аудиторные занятия - форма обучения очная 1 курс (2 семестр)

Название и разделов и тем	Всего	Виды аудиторных занятий	
		лекции	семинары / в т. ч. в интерактивной форме
Тема1.Объект, предмет и метод дисциплины.	4	2	2/2
Тема 2. Основные задачи и информационные технологии их решения в организации.	4	2	2/2
Тема 3 Основные угрозы информационной безопасности в организации[1].	4	2	2/2
Тема 4. Нормативное и методическое обеспечение информационной безопасности[2].	4	2	2
Тема 5. Организационные и инженерные методы защиты информации организации	8	2	6/4
Тема 6. Механизмы обеспечения информационной безопасности организации[3].	8	2	6/4
Тема 7. Криптографические методы и средства обеспечения информационной безопасности организации[4].	8	2	6/2
Тема 8. Антивирусные средства обеспечения информационной безопасности.	8	2	6/4
Итого	48	16	32/20

[1] Занятия по данной теме проводятся с использованием средств мультимедиатехнологий.
[2] Занятия по данной теме проводятся с использованием средств мультимедиатехнологий.
[3] Занятия по данной теме проводятся с использованием средств мультимедиатехнологий.
[4] Занятия по данной теме проводятся с использованием средств мультимедиатехнологий.

Самостоятельная работа слушателей охватывает 60 часа, в том числе по темам: Тема1 – 4 часа; Тема 2 – 8 часа; Тема 3 – 8 часа; Тема 4 – 10 часа; Тема 5 – 8 часов; Тема 6 – 8 часов; Тема 7 – 6 часов; Тема 8 – 8 часов;

Итого: 60 часа.

Самостоятельная работа слушателей охватывает 60 часа, в том числе по темам:

Тема1 – 4 часа;

Тема 2 – 8 часа;

Тема 3 – 8 часа;

Тема 4 – 10 часа;

Тема 5 – 16 часов;

Тема 6 – 6 часов;

Тема 7 – 8 часов;

Итого: 60 часа.

Для успешного освоения дисциплины предусмотрены различные образовательные технологии, которые обеспечивают достижение планируемых результатов обучения согласно основной образовательной программе, с учетом требований к объему занятий в интерактивной форме, а именно:

- *Работа в группах*
- *Контрольный тест*
- *Выступление в роли обучающего*
- *Решение ситуационных задач*
- *Раздаточные материалы*
- *Мультимедийные презентации*

5. Содержание курса.

Тема 1. Объект, предмет и метод дисциплины «Компьютерные технологии и информационная безопасность». Понятие информационной безопасности. Организация как информационная система. Типовая структура организации: информационные подсистемы в организации. Базовые методы анализа информационной безопасности: структурно-функциональные модели процессов обработки информации в организации.

Тема 2. Типовые задачи обработки информации в организации: передача, прием, модификация, хранение и поиск информации. Формы представления информации в организации. Специфика решения типовых задач обработки информации в зависимости от формы обрабатываемой информации.

Тема 3. Основные угрозы информационной безопасности в организации: нарушения целостности, нарушения конфиденциальности и нарушения доступности информации. Основные причины нарушения информационной безопасности и источники угроз информа-

ционной безопасности в зависимости от формы представления информации и применяемых технологий обработки

Тема 4. Нормативные акты РФ в сфере обеспечения информационной безопасности. Международные и отечественные стандарты, регламентирующие применение методов и средств в области информационной безопасности. Соответствие комплекса ограничений и рекомендаций нормативных и методических рекомендаций составу и сложности задач обработки информации в организации.

Тема 5. Механизмы обеспечения информационной безопасности организации в процессах электронной обработки данных в соответствии с рекомендациями международных и отечественных стандартов: идентификация, аутентификация, авторизация, контроль доступа, управление конфигурацией, управление рисками, аудит и мониторинг. Основные технологии построения защищенных систем. Инструментарий обеспечения информационной безопасности. Экономические аспекты защиты информации в организации. Информационные риски и издержки, связанные с защитой информации в организации.

Тема 6. Криптография и криптоаналитика. Шифрование как инструмент обеспечения конфиденциальности информации. Стандарты шифрования. Шифрование с открытым ключом. Цифровая электронная подпись.

Тема 7. Вирусное программное обеспечение. Разновидности вирусов. Основные антивирусные программы.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

Тема 1. Понятие информационной безопасности. (форма проведения - дискуссия).

Вопросы к теме: Организация как информационная система. Типовая структура организации: информационные подсистемы в организации. Базовые методы анализа информационной безопасности: структурно-функциональные модели процессов обработки информации в организации.

Тема 2. Типовые задачи обработки информации в организации (форма проведения - дискуссия).

Вопросы к теме: Формы представления информации в организации. Специфика решения типовых задач обработки информации в зависимости от формы обрабатываемой информации.

Тема 3 Основные угрозы информационной безопасности в организации (форма проведения - дискуссия)

Вопросы к теме: Основные причины нарушения информационной безопасности и источники угроз информационной безопасности в зависимости от формы представления информации и применяемых технологий обработки

Тема 4 Нормативные акты РФ в сфере обеспечения информационной безопасности. (форма проведения - семинар)

Вопросы к теме: Международные и отечественные стандарты, регламентирующие применение методов и средств в области информационной безопасности. Соответствие комплекса ограничений и рекомендаций нормативных и методических рекомендаций составу и сложности задач обработки информации в организации.

Тема 5 Механизмы обеспечения информационной безопасности организации.(форма проведения - дискуссия)

Вопросы к теме: Основные технологии построения защищенных систем. Инструментарий обеспечения информационной безопасности. Экономические аспекты защиты информации в организации. Информационные риски и издержки, связанные с защитой информации в организации.

Тема 6 Криптография и криптоаналитика. (форма проведения - дискуссия)

Вопросы к теме: Шифрование как инструмент обеспечения конфиденциальности информации. Стандарты шифрования. Шифрование с открытым ключом. Цифровая электронная подпись.

Тема 7 Вирусное программное обеспечение. (форма проведения – практическое занятие)

Вопросы к теме: Разновидности вирусов. Основные антивирусные программы.

7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

По данной дисциплине не предусмотрены.

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

По данной дисциплине не предусмотрены.

9. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

При самостоятельном изучении отдельных тем настоящей дисциплины следует особое внимание уделить общесистемным аспектам информационных процессов в организации. Самостоятельная работа по освоению различных аспектов информационной безопасности должна проводиться с учетом взаимовлияния различных методов и средств обеспечения информационной безопасности и учетом рисков различной природы. Следует особе внимание уделять интегральным аспектам информационной безопасности, в качестве которых в первую очередь необходимо принимать аспекты экономические, связанные с оценкой возможного ущерба, который может понести организация, а также со стоимостью применяемых организации технологий обеспечения информационной безопасности. Оценка различных информационных рисков, возникающих в процессе функционирования организации должна быть приоритетной.

10. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

10.1. Литература

1. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с.

2.Галатенко В.А. Основы информационной безопасности / Под ред. члена-корреспондента РАН В.Б. Бетелина – М.: ИНТУИТ.РУ «Интернет-Университет Информационных Технологий», 2003.

3. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2010. - 324 с.

4. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. - Ст. Оскол: ТНТ, 2010. - 384 с.

5. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2012. - 432 с.

6. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. - М.: АРТА, 2012. - 296 с.

7. Семененко, В.А. Информационная безопасность: Учебное пособие / В.А. Семененко. - М.: МГИУ, 2010. - 277 с.

8. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. - 416 с.

9. Ярочкин, В.И. Информационная безопасность: Учебник для вузов / В.И. Ярочкин. - М.: Акад. Проект, 2008. - 544 с.

10.2.Программное обеспечение

ОС Windows XP,108; MS Office; Антивирусные программы

5.3.Интернет-ресурсы:

http://bezopasnik.org/

http://habrahabr.ru/

http:/intuit.ru

11. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

– Аудитории для проведения лекционных и семинарских занятий, оснащенные проектором, ноутбуком, аудиооборудованием для просмотра видео (6 аудитория, актовый зал, 703, 709 и др. аудитории в корпусах по ул.Федерации, 29 и по ул. Пушкинская, 4а).

– Аудитории, оборудованные интерактивными досками (603, 611).

– Аудитории для проведения тестирования и самостоятельной работы студентов с выходом в интернет, комп.класс №1к (корпус по ул. Федерации, 29).

– Читальный зал (803 аудитория) с компьютеризированными рабочими местами для работы с электронными библиотечными системами, каталогом и т.д.

Приложение к рабочей программе
По дисциплине «Компьютерные технологии и информационная безопасность»
Специальность «Экономика (магистратура)»
Профиль «Экономическая безопасность организации»

Процесс изучения дисциплины направлен на формирование следующих компетенций:

готовность действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения (ОК-2);

способностью принимать организационно-управленческие решения (ОПК-3);

способностью готовить аналитические материалы для оценки мероприятий в области экономической политики и принятия стратегических решений на микро- и макроуровне (ПК-8);

способность анализировать и использовать различные источники информации для проведения экономических расчетов (ПК-9).

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Критерий оценивания – умение правильно отвечать на вопросы тестового задания
Показатель оценивания – процент верных ответов на вопросы тестового задания
Шкала оценивания – выделено 4 уровня оценивания компетенций:
– высокий – не менее 80% правильных ответов
– достаточный – не менее 60% правильных ответов
– пороговый – не менее 30% правильных ответов
– критический – менее 30% правильных ответов

ТЕСТОВЫЕ ЗАДАНИЯ

Какие существуют основные уровни обеспечения защиты информации?
1) законодательный
2) административный
3) программно-технический
4) физический
5) вероятностный
6) процедурный
7) распределительный
Физические средства защиты информации
1) средства, которые реализуются в виде автономных устройств и систем
2) устройства, встраиваемые непосредственно в аппаратуру АС или устройства,
которые сопрягаются с аппаратурой АС по стандартному интерфейсу
3) это программы, предназначенные для выполнения функций, связанных с защитой информации
4) средства, которые реализуются в виде электрических, электромеханических
электронных устройств
В чем заключается основная причина потерь информации, связанной с ПК?
1) с глобальным хищением информации
2) с появлением интернета
3) с недостаточной образованностью в области безопасности
Технические средства защиты информации
1) средства, которые реализуются в виде автономных устройств и систем
2) устройства, встраиваемые непосредственно в аппаратуру АС или устройства,
которые сопрягаются с аппаратурой АС по стандартному интерфейсу
3) это программы, предназначенные для выполнения функций, связанных с
защитой информации
4) средства, которые реализуются в виде электрических, электромеханических и электронных устройств
К аспектам ИБ относятся
1) дискретность
2) целостность
3) конфиденциальность
4) актуальность
5) доступность
Что такое криптология?
1) защищенная информация
2) область доступной информации
3) тайная область связи

Что такое несанкционированный доступ (нсд)?
1) Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа
2) Создание резервных копий в организации
3) Правила и положения, выработанные в организации для обхода парольной защиты
4) Вход в систему без согласования с руководителем организации
5) Удаление не нужной информации
Что такое целостность информации?
1) Свойство информации, заключающееся в возможности ее изменения любым субъектом
2) Свойство информации, заключающееся в возможности изменения только единственным пользователем
3) Свойство информации, заключающееся в ее существовании в виде единого набора файлов
4) Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию)
Кто является знаковой фигурой в сфере информационной безопасности
1) Митник
2) Шеннон
3) Паскаль
4) Беббидж
В чем состоит задача криптографа?
1) взломать систему защиты
2) обеспечить конфиденциальность и аутентификацию передаваемых сообщений
Под ИБ понимают
1) защиту от несанкционированного доступа
2) защиту информации от случайных и преднамеренных воздействий естественного и искуственного характера
3) защиту информации от компьютерных вирусов
Что такое аутентификация?
1) Проверка количества переданной и принятой информации
2) Нахождение файлов, которые изменены в информационной системе несанкционированно
3) Проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа).
4) Определение файлов, из которых удалена служебная информация
5) Определение файлов, из которых удалена служебная информация
"Маскарад"- это
1) осуществление специально разработанными программами перехвата имени и пароля
2) выполнение каких-либо действий одним пользователем от имени другого пользователя, обладающего соответствующими полномочиями
Верификация –
Выберите один из 3 вариантов ответа:
1) это проверка принадлежности субъекту доступа предъявленного им идентификатора.
2) проверка целостности и подлинности инф, программы, документа
3) это присвоение имени субъекту или объекту
Кодирование информации –
1) представление информации в виде условных сигналов с целью автоматизации ее хранения, обработки, передачи и т.д.
2) метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом
Утечка информации
1) несанкционированное изменение информации, корректное по форме, содержанию, но отличное по смыслу
2) ознакомление постороннего лица с содержанием секретной информации
3) потеря, хищение, разрушение или неполучение переданных данных
Под изоляцией и разделением (требование к обеспечению ИБ) понимают
1) разделение информации на группы так, чтобы нарушение одной группы
информации не влияло на безопасность других групп информации (документов)
2) разделение объектов защиты на группы так, чтобы нарушение защиты одной группы не влияло на безопасность других групп
К аспектам ИБ относятся
1) дискретность
2) целостность
3) конфиденциальность
4) актуальность
5) доступность
Линейное шифрование –

1) несанкционированное изменение информации, корректное по форме и содержанию, но отличное по смыслу
2) криптографическое преобразование информации при ее передаче по прямым каналам связи от одного элемента ВС к другому
3) криптографическое преобразование информации в целях ее защиты от ознакомления и модификации посторонними лицами
Прочность защиты в АС
1) вероятность не преодоления защиты нарушителем за установленный промежуток времени
2) способность системы защиты информации обеспечить достаточный уровень своей безопасности
3) группа показателей защиты, соответствующая определенному классу защиты
Уровень секретности – это
1) ответственность за модификацию и НСД информации
2) административная или законодательная мера, соответствующая мере ответственности лица за утечку или потерю конкретной секретной информации, регламентируемой специальным документом, с учетом государственных, военно-стратегических, коммерческих, служебных или частных интересов
Угроза – это
1) возможное событие, действие, процесс или явление, которое может привести к ущербу чьих-либо интересов
2) событие, действие, процесс или явление, которое приводит к ущербу чьих-либо интересов
Под ИБ понимают
1) защиту от несанкционированного доступа
2) защиту информации от случайных и преднамеренных воздействий естественного и искуственного характера
3) защиту информации от компьютерных вирусов
Что такое криптография?
1) метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом
2) область доступной информации
3) область тайной связи, с целью защиты от ознакомления и модификации посторонним лицом
Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, установленными собственником информации называется
1) кодируемой
2) шифруемой
3) недостоверной
4) защищаемой

ПЕРЕЧЕНЬ ЭКЗАМЕНАЦИОННЫХ ВОПРОСОВ

1. Что можно узнать по информации, хранящейся у вас в компьютере.
2. Методы запрета доступа к компьютеру при кратковременных отлучках.
3. Правила организации рабочего места с точки зрения безопасности.
4. Правила работы на компьютере с точки зрения безопасности.
5. Архивирование данных.
6. Способы повышения надежности хранения информации.
7. Безопасность при работе в Internet и сети.
8. Меры предосторожности при работе в сети Internet.
9. Электронная почта. Оценка в плане безопасности. Методы обеспечения безопасности.
10. Шифрование. Основные сведения.
11. Симметричное шифрование.
12. Ассиметричное шифрование.
13. Цифровая подпись. Назначение, области применения.
14. Файловые системы операционных систем фирмы Microsoft с точки зрения безопасности.
15. Операционные системы фирмы Microsoft с точки зрения безопасности.
16. Однонаправленные функции.
17. Хэш-функции.
18. Вирусы. Основные сведения.
19. Макросы.
20. Резидентные вирусы.
21. Полиморфные вирусы.
22. Загрузочные вирусы.
23. DIR-вирусы.
24. Вирусы спутники.
25. Троянские кони.
26. Вирусы-Черви.
27. Защита от вирусов на программном уровне.
28. Защита от вирусов средствами BIOS.
29. Пути проникновения вирусов в компьютер.
30. Причины распространения почтовых червей.
31. Экономика информационной безопасности.