

**Федеральное государственное бюджетное образовательное
учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА
И ГОСУДАРСТВЕННОЙ СЛУЖБЫ
ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»**

Институт экономики, математики и информационных технологий

Школа IT-менеджмента

(наименование структурного подразделения (института/факультета/филиала))

Системы управления бизнес-процессами

(наименование кафедры)

УТВЕРЖДЕНА

ученым советом

Института ЭМИТ

Протокол от «9» сентября 2020 г.

№ 1-20/21

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.01.01 Информационная безопасность руководителя

(индекс, наименование дисциплины, в соответствии с учебным планом)

краткое наименование дисциплины (при наличии)

38.04.02, Менеджмент

(код, наименование направления подготовки (специальности))

Информационный менеджмент

(направленность(и) (профиль (и)/специализация(ии))

магистр

(квалификация)

очно-заочная, заочная

(форма(ы) обучения)

Год набора - 2021

Москва, 2021 г.

Автор(ы)–составитель(и):

Старший преподаватель
кафедры Системы управления
бизнес-процессами

к.т.н, Котухов М.М.

Заведующий кафедрой
Системы управления бизнес-процессами

д.т.н., профессор Рыжов А.П.

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы
2. Объем и место дисциплины в структуре образовательной программы
3. Содержание и структура дисциплины
4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине
5. Методические указания для обучающихся по освоению дисциплины
6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине
 - 6.1. Основная литература
 - 6.2. Дополнительная литература
 - 6.3. Учебно-методическое обеспечение самостоятельной работы
 - 6.4. Нормативные правовые документы
 - 6.5. Интернет-ресурсы
 - 6.6. Иные источники
7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы

1.1. Дисциплина Б1.В.ДВ.01.01 «Информационная безопасность руководителя» обеспечивает овладение следующими компетенциями с учетом этапа:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПКо-1	Способность оценивать конкурентную среду и разрабатывать маркетинговую стратегию предприятия	1 этап (код этапа-ПКо-1.1)	Способность оценивать конкурентную и планировать маркетинговые мероприятия
ПКс-5	Способность управлять отношениями с поставщиками и потребителями ресурсов и сервисов ИТ	1 этап (код этапа-ПКс-5.1)	Контроль взаимоотношений с поставщиками и потребителями ресурсов и сервисов ИТ

1.2. В результате освоения дисциплины у студентов должны быть сформированы:

ОТФ/ТФ профессиональные действия	Код этапа освоения компетенции	Результаты обучения
	ПКо-1.1	<p>на уровне знаний: методы оценки конкурентной среды и основы операционного и стратегического маркетингового планирования</p> <p>на уровне умений: формировать операционный маркетинговый план предприятия</p> <p>на уровне навыков: оценки эффективности текущих маркетинговых планов предприятия и внесения корректировок в них в случае выявления недостаточной эффективности с использованием современных информационно-цифровых методов и средств</p>
Контроль взаимоотношений с поставщиками и потребителями ресурсов и сервисов ИТ	ПКс-5.1.	<p>на уровне знаний: Принципы и методики управления персоналом, Кадровый документооборот, Особенности управления персоналом ИТ, Профессиональные стандарты ИТ, Принципы взаимодействия с пользователями, заказчиками и поставщиками сервисов ИТ, Принципы и методы проведения совещаний и презентаций, Принципы и методики управления конфликтами</p> <p>на уровне умений: Мотивировать, обучать персонал и создавать условия для его развития,</p>

	<p>Управлять персоналом, в том числе осуществлять прием на работу и увольнение работников, Организовывать разработку и внедрять политики, регламенты, положения, должностные инструкции, Организовывать создание презентационных и маркетинговых материалов и проводить презентации, Взаимодействовать с пользователями, заказчиками и поставщиками, Оценивать и повышать удовлетворенность пользователей и заказчиков сервисов ИТ</p> <p>на уровне навыков: Формирование целей, приоритетов, обязанностей и полномочий персонала, обслуживающего ресурсы ИТ, Формирование организационной и функциональной структуры персонала, обслуживающего ресурсы ИТ, Построение эффективных коммуникаций между персоналом, обслуживающим ресурсы ИТ, и с заинтересованными лицами, Организация и мотивация персонала, обслуживающего ресурсы ИТ, для выполнения поставленных целей, Прием на работу и увольнение персонала, обслуживающего ресурсы ИТ, Контроль персонала, обслуживающего ресурсы ИТ, достижения им поставленных целей и выполнения задач, в том числе проведение аттестации персонала, Обучение и реализация мер по профессиональному развитию персонала, обслуживающего ресурсы ИТ, Формирование и согласование принципов взаимоотношений с пользователями и поставщиками сервисов ИТ, в частности принципов выбора поставщиков сервиса, Организация планирования и осуществления взаимоотношений, активное участие во взаимоотношениях с пользователями и поставщиками сервисов ИТ, Организация повышения компетенций пользователей и поставщиков сервисов ИТ в сервисах ИТ, Контроль взаимоотношений с пользователями и поставщиками сервисов ИТ и обеспечение их прозрачности для заинтересованных лиц, Оценка и анализ взаимоотношений с пользователями и поставщиками сервисов ИТ, получение обратной связи и выполнение управленческих действий по результатам анализа</p>
--	--

2. Объем и место дисциплины в структуре ОП ВО

Дисциплина «Информационная безопасность руководителя» относится к блоку Б1.В.ДВ «Дисциплины (модули). Вариативная часть. Дисциплины по выбору». Код дисциплины Б1.В.ДВ.01.01 Дисциплина изучается на 1 курсе, во 2 семестре. Общая трудоемкость дисциплины -108 (ЗЗЕ).

Содержание курса является логическим продолжением и развитием дисциплин:

Управление процессами, Стандарты управления ИТ

Количество академических часов, выделяемых на контактную работу с преподавателем составляет 16 часов, из них 16 – на практические занятия. На самостоятельную работу обучающихся отводится 92 часа.

Формой промежуточной аттестации в соответствии с учебным планом является зачет оценкой.

3. Содержание и структура дисциплины

Очно-заочная форма обучения

п/п	№	Наименование тем и/или разделов	Объем дисциплины, час.					Форма текущего контроля успеваемости**, промежуточной аттестации***	
			Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий					СР
				Л/ЭО, ДОТ*	ЛР/ ЭО, ДОТ*	ПЗ/ ЭО, ДОТ*	КС Р		
Тема 1		Роль и значение ИБ руководителя. Основные понятия ИБ	10			2		8	О
Тема 2		Законодательное и нормативное правовое обеспечение ИБ руководителя	14			2		12	О
Тема 3		Основы криптологии	14			2		12	О
Тема 4		Лицензирование и сертификация в области ИБ	14			2		12	О
Тема 5		Практические вопросы построения СУИБ	14			2		12	О
Тема 6		Аудит ИБ	14			2		12	О
Тема 7		Основные национальные и международные стандарты в области ИБ	14			2		12	О

Тема 8	Особенности защиты персональных данных	14			2		12	О
Промежуточная аттестация								Зачет с оценкой
Всего:		108			16		92	

О-опрос

Содержание дисциплины

Тема 1. Роль и значение ИБ руководителя. Основные понятия ИБ

Статистика информационных инцидентов. Основные направления атак на информационные ресурсы. Направления защиты информации. Основные регуляторы в области ИБ.

Тема 2. Законодательное и нормативное правовое обеспечение ИБ руководителя

Классификация шифров. Симметричные шифры. Асимметричные шифры. Смешанные шифры

Основы криптоанализа. Нормативная база ФСБ России и правила использования.

Тема 3. Основы криптологии

Классификация шифров. Симметричные шифры. Асимметричные шифры. Смешанные шифры. Основы криптоанализа. Нормативная база ФСБ России и правила использования

Тема 4. Лицензирование и сертификация в области ИБ

Виды лицензий в области ИБ. Лицензирование ФСТЭК России. Лицензирование ФСБ России. Направления совершенствования лицензирования в области ИБ.

Тема 5. Практические вопросы построения СУИБ

Принципы построения Службы ИБ. Структура Службы ИБ. Проблемные вопросы создания и функционирования Службы ИБ и их решение.

Тема 6. Аудит ИБ

Требования к аудиту. Виды аудита. Порядок проведения аудита ИБ.

Тема 7. Основные национальные и международные стандарты в области ИБ

Национальные стандарты и руководящие документы по ИБ. Основные международные стандарты по ИБ и их назначение. Сертификация на соответствие стандартам по ИБ.

Тема 8. Особенности защиты персональных данных

Требования по защите ПДн в ИСПДн. Порядок приведения ИСПДн в соответствие с требованиями регуляторов.

4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине

4.1. Формы и методы текущего контроля успеваемости обучающихся и промежуточной аттестации.

4.1.1. В ходе реализации дисциплины Б1.В.ДВ.01.01 «Информационная безопасность руководителя» используются следующие методы текущего контроля успеваемости обучающихся:

– при проведении практических занятий: опрос

4.1.2. Зачет проводится с применением следующих методов (средств):

Устный: ответить на вопросы

4.2. Вопросы, вынесенные на самостоятельное обучение

1. Анализ состава и полноты нормативных документов в своей организации
2. Составление перечня необходимых документов
3. Практическое освоение поиска источников нормативных документов в Интернете
4. Нормативная база ФСБ России и правила использования средств шифрования
5. Анализ имеющихся лицензий и сертификатов имеющихся СЗКИ в организации
6. Практическая работа с Единым реестром СЗКИ
7. Анализ существующего порядка и организации защиты информации в своей организации
8. Практическое освоение работы с источниками информации по национальным стандартам, руководящим документам ФСТЭК России и ФСБ России, а также международным стандартам по ИБ
9. Анализ существующего порядка и организации защиты ПДн в своей организации

4.3. Оценочные средства для промежуточной аттестации.

4.3.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы. Показатели и критерии оценивания компетенций с учетом этапа их формирования

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПКо-1	Способность оценивать конкурентную среду и разрабатывать маркетинговую стратегию предприятия	1 этап (код этапа-ПКо-1.1)	Способность оценивать конкурентную и планировать маркетинговые мероприятия
ПКс-5	Способность управлять отношениями с поставщиками и потребителями ресурсов и сервисов ИТ	1 этап (код этапа-ПКс-5.1)	Контроль взаимоотношений с поставщиками и потребителями ресурсов и сервисов ИТ

Этап освоения компетенции	Показатель оценивания	Критерий оценивания
ПКо-1.1. Способность оценивать конкурентную и планировать маркетинговые мероприятия	Освоение методов оценки конкурентной среды и основ операционного и стратегического маркетингового планирования	Знает методы оценки конкурентной среды и основы операционного и стратегического маркетингового планирования
ПКс-5.1. Контроль	Повышает уровень удовлетворенности	Достигнуты все поставленные цели в

Этап освоения компетенции	Показатель оценивания	Критерий оценивания
взаимоотношений с поставщиками и потребителями ресурсов и сервисов ИТ	пользователей и заказчиков ресурсов и сервисов ИТ	переговорах с пользователями и заказчиками ресурсов и сервисов ИТ

4.3.2 Типовые оценочные средства

№ п/п	В О П Р О С	Варианты ответа
1.	Какие грифы секретности разрешено использовать для носителей сведений, составляющих гос. тайну?	<input type="checkbox"/> - Особой важности <input type="checkbox"/> - Совершенно секретно <input type="checkbox"/> - Секретно <input type="checkbox"/> - Для служебного пользования <input type="checkbox"/> - Конфиденциально
2.	Разрешено ли использование грифов секретности для документов, не содержащих сведения, отнесенные к гос. тайне?	<input type="checkbox"/> - Да <input type="checkbox"/> - Нет
3.	Кто уполномочен выдавать лицензии на работу со сведениями, составляющими гос. тайну?	<input type="checkbox"/> - Управление ФСБ России по ФО <input type="checkbox"/> - ЦЛСЗГТ ФСБ России <input type="checkbox"/> - ФСТЭК России
4.	Кто определяет режим защиты конфиденциальной информации?	<input type="checkbox"/> - Уполномоченный гос. орган <input type="checkbox"/> - Собственник информации
5.	Требуется ли обязательная сертификация средств обработки и защиты документированной информации с ограниченным доступом не составляющей гос. тайну?	<input type="checkbox"/> - Да <input type="checkbox"/> - Нет
6.	Сколько определено уровней возможностей нарушителей, имеющих доступ к работе с АС и СВТ по РД ФСТЭК России ?	<input type="checkbox"/> - Три <input type="checkbox"/> - Четыре <input type="checkbox"/> - Пять
7.	Сколько определено классов защищенности средств вычислительной техники по РД ФСТЭК России ?	<input type="checkbox"/> - Пять <input type="checkbox"/> - Шесть <input type="checkbox"/> - Семь
8.	Сколько определено классов защищенности автоматизированных систем по РД ФСТЭК России?	<input type="checkbox"/> - Шесть <input type="checkbox"/> - Семь <input type="checkbox"/> - Восемь <input type="checkbox"/> - Девять
9.	Сколько определено уровней контроля отсутствия недеklarированных возможностей программных средств по РД ФСТЭК России ?	<input type="checkbox"/> - Четыре <input type="checkbox"/> - Пять <input type="checkbox"/> - Шесть <input type="checkbox"/> - Семь
10.	Сколько определено оценочных уровней доверия в соответствии с ГОСТ Р ИСО/МЭК 15408-2002?	<input type="checkbox"/> - Четыре <input type="checkbox"/> - Пять <input type="checkbox"/> - Шесть <input type="checkbox"/> - Семь

№ п/п	В О П Р О С	Варианты ответа
11.	Сколько определено классов защищенности государственных информационных систем (ГИС)?	<input type="checkbox"/> - Три <input type="checkbox"/> - Четыре
12.	Сколько определено уровней защищенности информационных систем персональных данных (ИСПДн)?	<input type="checkbox"/> - Три <input type="checkbox"/> - Четыре <input type="checkbox"/> - Пять
13.	Какую лицензию надо получить для выполнения работ по защите конфиденциальной информации в АС, не использующих средств шифрования?	<input type="checkbox"/> - Лицензию Управления ФСБ России по ФО <input type="checkbox"/> - Лицензию ЦЛСЗГТ ФСБ России <input type="checkbox"/> - Лицензию ФСТЭК России
14.	Какую лицензию надо получить для выполнения работ по разработке средств защиты конфиденциальной информации с использованием средств шифрования?	<input type="checkbox"/> - Лицензию Управления ФСБ России по ФО <input type="checkbox"/> - Лицензию ЦЛСЗГТ ФСБ России <input type="checkbox"/> - Лицензию ФСТЭК России
15.	Является ли обязательным использование сертифицированных средств защиты конфиденциальной информации, отнесенной к охраняемой законом информации?	<input type="checkbox"/> - Да <input type="checkbox"/> - Нет
16.	Сертифицируются ли СЗИ, созданные организациями, не имеющими лицензий?	<input type="checkbox"/> - Да <input type="checkbox"/> - Нет
18.	Является ли обязательным одобрение ФСБ России алгоритма криптозащиты до его реализации?	<input type="checkbox"/> - Да <input type="checkbox"/> - Нет
19.	Могут ли приниматься на сертификацию импортные средства защиты информации, не использующие встроенные шифровальные алгоритмы и средства?	<input type="checkbox"/> - Да <input type="checkbox"/> - Да, от имени отечественных компаний <input type="checkbox"/> - Нет
20.	Могут ли приниматься на сертификацию импортные шифровальные алгоритмы и средства?	<input type="checkbox"/> - Да <input type="checkbox"/> - Да, от имени отечественных компаний <input type="checkbox"/> - Нет
21.	Укажите алгоритмы шифрования, использующие симметричные методы шифрования (с секретным ключом).	<input type="checkbox"/> - DES <input type="checkbox"/> - Triple DES <input type="checkbox"/> - IDEA <input type="checkbox"/> - RSA <input type="checkbox"/> - El Gamal <input type="checkbox"/> - PGP <input type="checkbox"/> - ГОСТ 28147-89
22.	Укажите алгоритмы шифрования, использующие асимметричные методы (с открытым ключом).	<input type="checkbox"/> - DES <input type="checkbox"/> - Triple DES <input type="checkbox"/> - IDEA <input type="checkbox"/> - RSA <input type="checkbox"/> - El Gamal <input type="checkbox"/> - PGP <input type="checkbox"/> - ГОСТ 28147-89

Шкала оценивания.

Шкала оценивания

Уровень	Критерии	Баллы
Высокий	Студент показывает отличные знания изученного учебного материала; самостоятельно, логично и последовательно излагает и интерпретирует материалы учебного курса; полностью раскрывает смысл предлагаемого вопроса; владеет основными терминами и понятиями изученного курса; показывает умение переложить теоретические знания на предполагаемый практический опыт	41-50
Хороший	Студент показывает хорошие знания изученного учебного материала; самостоятельно, логично и последовательно излагает и интерпретирует материалы учебного курса; почти полностью раскрывает смысл предлагаемого вопроса; владеет основными терминами и понятиями изученного курса; в основном показывает умение переложить теоретические знания на предполагаемый практический опыт	31-40 21-30
Средний	Студент показывает не очень хорошие знания изученного учебного материала; слабо излагает и интерпретирует материалы учебного курса; кратко раскрывает смысл предлагаемого вопроса; владеет основными терминами и понятиями изученного курса; практически отсутствует умение переложить теоретические знания на предполагаемый практический опыт	11-20
Низкий	При наличии серьезных упущений в процессе изложения учебного материала; в случае отсутствия знаний основных понятий и определений курса или присутствии большого количества ошибок при интерпретации основных определений; если студент показывает значительные затруднения при ответе на предложенные основные и дополнительные вопросы; при условии отсутствия ответа на основной и дополнительный вопросы	10 балл и ниже

Максимальное количество баллов, которое студент может набрать в процессе обучения в рамках учебного курса – **100 баллов**:

91-100 баллов	зачтено	(А)
81-90 баллов	зачтено	(В)
71-80 баллов	зачтено	(С)
61-70 баллов	зачтено	(D)
60 и менее	незачтено	(Е).

4.4. Методические материалы

В части обеспечения освоения дисциплины обучающимся предоставляется раздаточный материал по темам дисциплины.

Процедура оценивания знаний, умений и навыков, обеспечивающих формирование компетенций, предусмотренных освоением дисциплины, включает:

- проведение опроса по ключевым вопросам, охватывающем содержание дисциплины.

5. Методические указания для обучающихся по освоению дисциплины

Для обеспечения освоения дисциплины обучающиеся учебным планом предусмотрена самостоятельная работа и практические занятия.

Виды самостоятельной внеаудиторной работы:

- самостоятельное изучение разделов курса,
- повторение раздаточного материала,
- подготовка к практическим занятиям,
- подготовка к текущему контролю.

6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Основная литература.

1. Афонин, А.М. Управление проектами: Учебное пособие / А.М. Афонин, Ю.Н. Информационная безопасность. Учебник для вузов /Котухов М.М. и др., - М.: Изд. МФТИ, 2009. – 269 с.
2. Бабащ, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабащ, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с.
3. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2010. - 324 с.

6.2. Дополнительная литература.

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. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. - М.: ЮНИТИ-ДАНА, 2013. - 239 с.
6. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2012. - 432 с.
7. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. - М.: АРТА, 2012. - 296 с.
8. Семененко, В.А. Информационная безопасность: Учебное пособие / В.А. Семененко. - М.: МГИУ, 2010. - 277 с.

6.4. Нормативные правовые документы.

1. Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных"

6.5. Интернет-ресурсы.

1. Сайты ФСТЭК России, ФСБ России, Роскомнадзора.

6.6. Иные источники.

1. Система Гарант <http://www.garant.ru/>
2. Консультант Плюс <http://www.consultant.ru/>

7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

Для проведения занятий по дисциплине необходимо материально-техническое обеспечение учебных аудиторий (наглядными материалами, экраном, мультимедийным проектором с ноутбуками (ПК) для презентации учебного материала, выходом в сеть Интернет, программными продуктами Microsoft Office (Excel, Word, PowerPoint)) в зависимости от типа занятий: семинарского и лекционного типов, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Для самостоятельной работы обучающимся необходим доступ в читальные залы библиотеки и/или помещение, оснащенное компьютерной техникой с возможностью

подключения к сети «Интернет», доступ в электронную информационно-образовательную среду организации и ЭБС.

Информационные справочные системы:

1. Информационно-правовой портал «Консультант плюс» (правовая база данных). [Электронный ресурс]. – URL: <http://www.consultant.ru/>
2. Информационно-правовой портал «Гарант» (правовая база данных). [Электронный ресурс]. – URL: <http://www.garant.ru/>
3. Научная библиотека РАНХиГС. URL: <http://lib.ranepa.ru/>;
4. Научная электронная библиотека eLibrary.ru. URL: <http://elibrary.ru/defaultx.asp>;
5. Национальная электронная библиотека. URL: <http://rusneb.ru>;
6. Российская государственная библиотека. URL: www.rsl.ru;
7. Российская национальная библиотека. URL: <http://nlr.ru/>;
8. Электронная библиотека Grebennikon. URL: <http://grebennikon.ru/>;
9. Электронно-библиотечная система Издательства «Лань». URL: <http://e.lanbook.com>;
10. Электронно-библиотечная система ЮПАЙТ. URL: <http://www.biblio-online.ru/>;
11. Электронно-библиотечная система IPRbooks. URL: <http://www.iprbookshop.ru/>