

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

ИНСТИТУТ ОТРАСЛЕВОГО МЕНЕДЖМЕНТА

**Факультет инженерного менеджмента
Кафедра теории и систем отраслевого управления**

УТВЕРЖДЕНА
кафедрой теории и систем
отраслевого управления
Протокол от «28» августа 2019 г.
№1

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.09 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

направление подготовки
38.04.02 Менеджмент

направленность (профиль):
«Технологическое предпринимательство»

квалификация (степень) выпускника
магистр

форма обучения
очная

Год набора - 2020

Москва, 2019 г.

Автор–составитель:

д.э.н. профессор, профессор кафедры теории и систем отраслевого управления

Минченкова О.Ю.

ассистент кафедры теории и систем отраслевого управления Иванов В.Ю.

Заведующий кафедрой теории и систем отраслевого управления к.э.н., доцент
Серебренников С.С.

СОДЕРЖАНИЕ

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ.....	4
2. ОБЪЕМ И МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ.....	6
3. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ.....	6
4. МАТЕРИАЛЫ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ ОБУЧАЮЩИХСЯ И ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ.....	9
4.1. Текущий контроль успеваемости.....	9
4.1.1. <i>Формы текущего контроля успеваемости.....</i>	<i>9</i>
4.1.2. <i>Материалы текущего контроля успеваемости.....</i>	<i>9</i>
4.2. Промежуточная аттестация.....	12
4.2.1. <i>Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы. Показатели и критерии оценивания компетенций с учетом этапа их формирования.....</i>	<i>12</i>
4.2.2. <i>Форма и средства проведения промежуточной аттестации.....</i>	<i>13</i>
4.2.3. <i>Типовые оценочные средства.....</i>	<i>13</i>
4.3. Методические материалы.....	13
5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ.....	14
6. УЧЕБНАЯ ЛИТЕРАТУРА И РЕСУРСЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ "ИНТЕРНЕТ", УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ.....	19
6.1. Основная литература.....	19
6.2. Дополнительная литература.....	19
6.3. Учебно-методическое обеспечение самостоятельной работы.....	19
6.4. Нормативные правовые документы.....	20
6.5. Интернет-ресурсы.....	20
7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ.....	21

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

1.1. Дисциплина Б1.В.09 «Информационная безопасность» обеспечивает овладение следующими компетенциями с учетом этапа:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-2	Способность разрабатывать корпоративную стратегию, программы организационного развития и изменений и обеспечивать их реализацию	ПК-2.1	Способность анализировать действующую корпоративную стратегию, программы организационного развития и изменений

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

Обобщенные трудовые функции и трудовые функции	Код этапа освоения компетенции	Результаты обучения
Профессиональный стандарт Менеджер по информационным технологиям Обобщенные трудовые функции В. Управление сервисами ИТ Трудовые функции В/07.7 Управление непрерывностью сервисов ИТ Профессиональный стандарт Руководитель проектов в области информационных технологий Обобщенные трудовые функции В. Управление проектами в области ИТ малого и среднего уровня сложности в условиях неопределенностей, порождаемых запросами на изменения, с применением формальных инструментов управления рисками и проблемами проекта Трудовые функции В/49.7 Принятие мер по неразглашению информации, полученной от заказчика в проектах малого и среднего уровня сложности в области ИТ	ПК-2.1	<u>на уровне знаний:</u> <ul style="list-style-type: none"> • владеет профессиональной терминологией в области информационной безопасности • дает характеристику методам формирования требований по защите информации • знает принципы обеспечения режима секретности • знает правовые основы создания службы защиты информации в организации;
		<u>на уровне умений:</u> <ul style="list-style-type: none"> • определяет основания и процедуру осуществления защиты информации • анализирует и оценивает угрозы информационной безопасности объекта • оценивает уровень вовлеченности заинтересованных сторон в процесс обеспечения информационной безопасности • способствует обеспечению информационной безопасности в условиях глобализации информационного пространства • определяет основания и размеры ответственности за нарушения в сфере защиты информации • применяет отечественные и

		зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем
		<u>на уровне навыков:</u> <ul style="list-style-type: none"> • выделяет основания и объекты защиты информации

2. Объем и место дисциплины в структуре образовательной программы

Место дисциплины

Дисциплина Б1.В.09 «Информационная безопасность» относится к обязательным дисциплинам вариативной части образовательной программы подготовки магистров по направлению 38.04.02 «Менеджмент» (направленность (профиль) «Технологическое предпринимательство» и изучается в 3 семестре.

Объем дисциплины

Трудоемкость дисциплины оценивается в 3 ЗЕТ (108 академических часа/81 астрономических часов). На контактную работу с преподавателем в форме лекционных занятий отводится (6 академических часов/4,5 астрономических часа), в форме практических занятий – (26 академических часа/19,5 астрономических часа). На самостоятельную работу обучающихся отводится (76 академических часов/57 астрономических часа)

3. Содержание и структура дисциплины

№	Наименование тем и/или разделов	Объем дисциплины, ак.						Форма текущего контроля успеваемости, промежуточной аттестации
		всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
Тема 1	Теоретические основы информационной безопасности	18	2		4		12	О
Тема 2	Обеспечение информационной безопасности в условиях глобализации информационного пространства	19	1		4		14	К
Тема 3	Правовые режимы обеспечения безопасности информации ограниченного доступа	17	1		4		12	ПО
Тема 4	Юридическая ответственность за правонарушения в информационной сфере	18			6		12	Э
Тема 5	Проектирование систем защиты информации	19	1		4		14	Т
Тема 6	Анализ и управление рисками в сфере информационной безопасности	17	1		4		12	Т
Промежуточная аттестация		3а						
Всего:		108	6		26		76	

Условные обозначения: опрос(Э), кейс(К), письменный опрос(ПО), эссе(Э), тестирование(Т), зачет (3а)

Содержание дисциплины

Тема 1. Теоретические основы информационной безопасности.

Предмет и задачи теории защиты информации. Базовые термины и определения. Классификация угроз безопасности. Интерпретация угрозы атаки. Понятие надежности безопасности, параметры и характеристики безопасности. Классификация угроз уязвимостей и уровней защиты (защищенности). Объекты защиты и объекты моделирования.

Общая схема процесса обеспечения безопасности. Идентификация, аутентификация, управление доступом. Защита от несанкционированного доступа. Модели безопасности. Процесс построения и оценки системы обеспечения безопасности. Стандарт ISO/IEC 15408.

Тема 2. Обеспечение информационной безопасности в условиях глобализации информационного пространства

Информационная безопасность в информационном обществе. Современное информационное противоборство и обеспечение информационной безопасности.

Информационная безопасность в системе национальной безопасности Российской Федерации. Базовые принципы обеспечения информационной безопасности. Правовое регулирование информационной безопасности в системе российского информационного права. Правовые средства обеспечения безопасности информационной инфраструктуры Российской Федерации. Правовые средства обеспечения безопасности информации. Организационное обеспечение информационной безопасности Российской Федерации.

Тема 3. Правовые режимы обеспечения безопасности информации ограниченного доступа

Ограничение доступа к информации в целях защиты интересов личности, общества и государства. Правовые режимы тайн в системе организационного и правового обеспечения безопасности информации ограниченного доступа. Правовой режим защиты государственной тайны. Правовой режим коммерческой тайны. Правовой режим обеспечения безопасности персональных данных. Актуальные вопросы режима служебной тайны.

Противодействие экстремистской деятельности в информационной сфере. Защита детей от информации, причиняющей вред их здоровью и развитию. Правовые проблемы обеспечения информационной безопасности в сети Интернет

Тема 4. Юридическая ответственность за правонарушения в информационной сфере.

Понятие и виды юридической ответственности в области обеспечения информационной безопасности. Субъекты и объекты правоотношений в области обеспечения информационной безопасности. Преступность в информационной сфере как угроза информационной безопасности при формировании информационного общества в условиях глобализации. Проблемы уголовно-правовой ответственности за информационные преступления. Проблемы международного сотрудничества и зарубежный опыт противодействия преступлениям в информационной сфере

Тема 5. Проектирование систем защиты информации

Основополагающие методы и абстрактные модели контроля доступа. Абстрактные модели контроля доступа к защищенным режимам обработки информации. Модели и методы ролевого и сессионного контроля доступа. Вопросы идентификации ролей и сессий. Задачи построения системы защиты информации. Альтернативные методы защиты информации.

Стадии и задачи проектирования. Определение функциональных задач системы защиты информации. Определение требований к качеству разработки и технического сопровождения системы защиты информации. Экономическое обоснование проектных решений. Оценка производительности системы защиты информации. Эксплуатационное проектирование системы защиты информации.

Тема 6. Анализ и управление рисками в сфере информационной безопасности

Управление рисками. Модель безопасности с полным перекрытием. Управление

информационной безопасностью. Стандарты ISO/IEC 17799/27002 и 27001. Методики построения систем защиты информации. Методики и программные продукты для оценки рисков. Выбор проекта системы обеспечения информационной безопасности. Игровая модель конфликта «защитник-нарушитель».

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

4.1. Текущий контроль успеваемости

4.1.1. Формы текущего контроля успеваемости

В ходе реализации дисциплины Б1.В.09 «Информационная безопасность» текущий контроль успеваемости проводится в устной и письменной формах. Используются следующие методы текущего контроля успеваемости обучающихся:

№	Наименование тем и/или разделов	Методы текущего контроля успеваемости
Тема 1	Теоретические основы информационной безопасности	О
Тема 2	Обеспечение информационной безопасности в условиях глобализации информационного пространства	К
Тема 3	Правовые режимы обеспечения безопасности информации ограниченного доступа	ПО
Тема 4	Юридическая ответственность за правонарушения в информационной сфере	Э
Тема 5	Проектирование систем защиты информации	Т
Тема 6	Анализ и управление рисками в сфере информационной безопасности	Т

Условные обозначения: опрос(Э), кейс(К), письменный опрос(ПО), эссе(Э), тестирование(Т), зачет (За)

4.1.2. Материалы текущего контроля успеваемости

Типовые вопросы к устному опросу №1

1. Что такое информационная безопасность?
2. Перечислите основные угрозы информационной безопасности.
3. Какие существуют модели информационной безопасности?
4. Какие основные международные стандарты в области информационной безопасности существуют?
5. Как связаны международные стандарты и стандарты РФ?
6. Какие основные стандарты РФ в области информационной безопасности существуют?

Типовой кейс по теме №2

Кейс: «Как, зная только имя и email человека, злоумышленники получили доступ ко всем его аккаунтам и удаленно уничтожили информацию на всех его устройствах»

Источник: <https://habrahabr.ru/post/149179/>

Дата публикации статьи: 7.08.2012

«Очень интересная статья появилась сегодня на wired.com. Буквально за один час у автора статьи Мэта Хонана были взломаны Amazon, GMail, Apple и Twitter аккаунты и была удаленно уничтожена информация на его iPad, iPhone и MacBook. Среди прочего он потерял все фотографии своей дочки с ее рождения, многие документы и большую часть переписки. Очень интересно в этой истории то, как злоумышленник получил доступ к Amazon аккаунту и AppleID — для этого не понадобилась ничего, кроме доступной в сети информации и телефона.

Злоумышленнику приглянулся трехбуквенный Twitter Мэта. С целью заполучить его, он провел небольшое исследование, в ходе которого обнаружил, что Twitter аккаунт Мэта содержал ссылку на его личный сайт, который, в свою очередь, содержал его GMail адрес. Имея GMail адрес, злоумышленник начал процесс восстановления пароля. Так как двухступенчатая авторизация у Мэта включена не была, гугл на первом экране

восстановления пароля предоставил любезно обфусцированный альтернативный адрес: m****n@me.com. Сопоставив этот паттерн с gmail-адресом mhonan@gmail.com, злоумышленник получил Apple-овский email автора.

Первое, что было необходимо злоумышленнику для того, чтобы приступить к интересной части, это адрес Мэта, который легко обнаружился WhoIs сервисом в информации о его личном сайте. Имея адрес, злоумышленник позвонил в Амазон и сказал, что он владелец аккаунта и хочет добавить новую кредитную карту. Чтобы проверить, что злоумышленник действительно владелец аккаунта, Амазон спросил адрес, имя и email — вся эта информация у злоумышленника уже была, и он успешно ввел номер несуществующей кредитной карты, заблаговременно сгенерированный на одном из специализированных сайтов.

Затем он позвонил в Amazon опять, и сказал, что потерял доступ к своему Amazon аккаунту. Amazon попросил имя, адрес и номер кредитной карты. После предоставления этой информации (добавленный на предыдущем шаге номер кредитной карты подошел), злоумышленник смог добавить новый email адрес к аккаунту, на который восстановил пароль. В амазон аккаунте можно посмотреть список сохраненных кредиток, где, в целях безопасности, показываются только последние четыре цифры номера.

Затем злоумышленник звонит в AppleCare, где его спрашивают имя, адрес и последние четыре цифры кредитной карты, и выдают ему временный пароль на .me аккаунт. На этот аккаунт злоумышленник восстанавливает пароль от GMail, а на GMail пароль от Twitter. Используя AppleId он также удаляет всю информацию с iPhone, iPad и MacBook используя сервисы Find My Phone и Find My Mac. Печальный конец истории.

Позже Мэт связался с Apple, где ему сказали, что в данном конкретном случае внутренний регламент не был соблюден в полной мере, и что Apple относится к безопасности пользователей очень серьезно. Амазону тоже был отправлен запрос от Wired, но пока что ответа не последовало.

Сегодня, спустя три дня после того, как все это произошло, ребята из Wired за несколько минут смогли целиком повторить весь фокус дважды — от адреса и имени до доступа к Amazon и Apple аккаунтам со всеми вытекающими последствиями.»

Вопросы:

1. Какие недостатки в информационной инфраструктуре вы можете выделить?
2. Можно ли было избежать компрометации достаточного для взлома персональной информации?

Типовые вопросы к письменному опросу по теме №3

1. Какие основные законы в области защиты информации в РФ?
2. Перечислите основные цели и задачи РФ в области обеспечения информационной безопасности
3. Что такое концепция информационной безопасности?
4. Что такое конфиденциальная информация?
5. Что такое персональные данные?
6. В каких случаях возможно использовать персональные данные без согласия обладателя? Охарактеризуйте биометрические данные как персональные данные.
7. Что такое профессиональная тайна?
8. Что такое коммерческая тайна?
9. Что такое режим коммерческой тайны?
10. Что такое государственная тайна?
11. Опишите правовой режим государственной тайны.
12. Какие государственные органы занимаются сертификацией и лицензированием средств защиты информации?

Типовые темы эссе по теме №4

1. Актуальные проблемы уголовно-правовой борьбы с посягательствами на компьютерную информацию

2. Преступность в информационной сфере как угроза информационной безопасности при формировании информационного общества в условиях глобализации

Типовые тестовые вопросы по теме №5

1. Кто является основным ответственным за определение уровня классификации информации?
- A. Руководитель среднего звена
 - B. Высшее руководство
 - C. Владелец
 - D. Пользователь
2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
- A. Сотрудники
 - B. Хакеры
 - C. Атакующие
 - D. Контрагенты (лица, работающие по договору)
3. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?
- A. Поддержка высшего руководства
 - B. Эффективные защитные меры и методы их внедрения
 - C. Актуальные и адекватные политики и процедуры безопасности
 - D. Проведение тренингов по безопасности для всех сотрудников
4. Что такое политики безопасности?
- A. Пошаговые инструкции по выполнению задач безопасности
 - B. Общие руководящие требования по достижению определенного уровня безопасности
 - C. Широкие, высокоуровневые заявления руководства
 - D. Детализированные документы по обработке инцидентов безопасности
5. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?
- A. Анализ рисков
 - B. Анализ затрат / выгоды
 - C. Результаты ALE
 - D. Выявление уязвимостей и угроз, являющихся причиной риска

Типовые тестовые вопросы по теме №6

1. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?
- A. Чтобы убедиться, что проводится справедливая оценка
 - B. Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
 - C. Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа
 - D. Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку
2. Что из перечисленного не является целью проведения анализа рисков?
- A. Делегирование полномочий
 - B. Количественная оценка воздействия потенциальных угроз
 - C. Выявление рисков
 - D. Определение баланса между воздействием риска и стоимостью необходимых контрмер
3. Как рассчитать остаточный риск?

- A. Угрозы x Риски x Ценность актива
 B. (Угрозы x Ценность актива x Уязвимости) x Риски
 C. $SLE \times Частота = ALE$
 D. (Угрозы x Уязвимости x Ценность актива) x Недостаток контроля
4. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?
- A. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
 B. Когда риски не могут быть приняты во внимание по политическим соображениям
 C. Когда необходимые защитные меры слишком сложны
 D. Когда стоимость контрмер превышает ценность актива и потенциальные потери
5. Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?
- A. Много информации нужно собрать и ввести в программу
 B. Руководство должно одобрить создание группы
 C. Анализ рисков не может быть автоматизирован, что связано с самой природой оценки
 D. Множество людей должно одобрить данные

4.2. Промежуточная аттестация

4.2.1. 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
ПК-2	Способность разрабатывать корпоративную стратегию, программы организационного развития и изменений и обеспечивать их реализацию	ПК-2.1	Способность анализировать действующую корпоративную стратегию, программы организационного развития и изменений

Этап освоения компетенции	Показатель оценивания	Критерий оценивания
ПК-2.1	<ul style="list-style-type: none"> исследует корпоративную стратегию типовой организации (на примере бизнес-кейса) определяет соответствие действующей корпоративной стратегии, программ организационного развития и изменений запросам заинтересованных сторон анализирует эффективность исполнения действующей программы организационного развития 	<ul style="list-style-type: none"> проанализирована стратегия управления интеллектуальной собственностью и подготовлены предложения по совершенствованию системы ее защиты выявлены все заинтересованные стороны проекта, процесса или организации и определены возможные факторы проявления структурной инерции проведен анализ

	и изменений	<p>удовлетворенности 3 и более сторон заинтересованных сторон (включая клиентов, правительственные учреждения, работников, собственников и акционеров) действующей корпоративной стратегии, программой организационного развития и изменений</p> <ul style="list-style-type: none"> • сформулированы не менее 5 критериев оценки эффективности исполнения действующей программы организационного развития и изменений
--	-------------	--

4.2.2. Форма и средства проведения промежуточной аттестации

По дисциплине Б1.В.09 «Информационная безопасность» учебным планом предусмотрен зачет, который проводится в письменной форме в виде анализа бизнес-ситуаций. Все 2 задания направлены на проверку качества освоения компетенции ПК-2.1.

4.2.3. Типовые оценочные средства

Типовой билет к зачету

Билет №1

1. Проанализируйте регламент по информационной безопасности в компании ____¹. Оцените уровень вовлеченности заинтересованных сторон в процесс обеспечения информационной безопасности.
2. Какие действия стоит предпринять компании для повышения эффективности управления информационной безопасностью?

Билет №2

1. Проанализируйте регламент по информационной безопасности в компании ____². Оцените уровень вовлеченности заинтересованных сторон в процесс обеспечения информационной безопасности.
2. Какие наиболее слабые места в управления информационной безопасностью вы можете назвать? Почему иногда невозможно нейтрализовать все угрозы.

4.3. Методические материалы

Промежуточная аттестация по дисциплине Б1.В.09 «Информационная безопасность» проводится в письменной форме в виде анализа бизнес-ситуаций. Все вопросы билета предполагают ответ студентом на вопросы, связанные с информационной безопасностью компании.

На выполнение заданий студенту отводится 40 минут. После проверки преподавателем ответов на каждое задание студенту могут быть заданы дополнительные уточняющие вопросы. В случае если студент при ответе допустил несущественные неточности, ему могут быть заданы дополнительные вопросы на сходную тему.

Шкала оценивания для промежуточной аттестации

Оценка	Требования к знаниям
«зачтено»	Оценка «зачтено» выставляется, если студентом: 1. оценен уровень вовлеченности заинтересованных сторон в процесс обеспечения информационной безопасности 2. продемонстрирована способность содействовать обеспечению информационной безопасности в условиях глобализации информационного пространства
«не зачтено»	Оценка «не зачтено» выставляется студенту, если студентом задание выполнено не в полном объеме и на недостаточном уровне

¹ Название компании устанавливается в зависимости от перечня рассмотренных в течение семестра кейсов

² Название компании устанавливается в зависимости от перечня рассмотренных в течение семестра кейсов

5. Методические указания для обучающихся по освоению дисциплины

Процесс обучения по дисциплине Б1.В.09 «Информационная безопасность» включает следующие основные виды занятий:

1. лекции;
2. практические занятия;
3. самостоятельная работа.

На лекциях студенты изучают основные теоретические концепции защиты информации и нормативно-правовое регулирование информационной безопасности, знакомятся с наиболее известными работами ученых и существующими практическими разработками в данной области, закрепляя полученные знания на практических занятиях. С целью обеспечения успешного обучения студенту необходимо готовиться к каждой лекции, т.к. она является важнейшей формой организации учебного процесса, поскольку знакомит с новым учебным материалом, разъясняет учебные элементы, трудные для понимания, систематизирует учебный материал, ориентирует в учебном процессе.

Подготовку к лекции рекомендуется проводить по следующему плану:

1. внимательно прочитайте материал предыдущей лекции;
2. узнайте тему предстоящей лекции (по тематическому плану, по информации лектора);
3. ознакомьтесь с учебным материалом по учебнику и учебным пособиям;
4. постарайтесь уяснить место изучаемой темы в своей профессиональной подготовке;
5. запишите возможные вопросы, которые вы зададите лектору на лекции

Практические занятия предполагают выполнение различного вида работ: разбор типовых ситуаций, решение аналитических задач, выполнение тестов.

Подготовку к практическому занятию рекомендуется проводить по следующему плану:

1. внимательно прочитайте материал лекций относящихся к данному семинарскому занятию, ознакомьтесь с учебным материалом по учебнику и учебным пособиям;
2. выпишите основные термины;
3. ответьте на контрольные вопросы по семинарским занятиям, готовьтесь дать развернутый ответ на каждый из вопросов;
4. уясните, какие учебные элементы остались для вас неясными и постарайтесь получить на них ответ заранее (до семинарского занятия) во время текущих консультаций преподавателя;
5. готовиться можно индивидуально, парами или в составе малой группы, последние являются эффективными формами работы;

Получение углубленных знаний по изучаемой дисциплине достигается за счет дополнения часов аудиторной нагрузки самостоятельной работой студентов, которая выражается в анализе дополнительной литературы по учебной дисциплине и подготовке реферативных материалов по отдельным темам учебной программы. При изучении дисциплины предусматривается обеспечение гармоничной взаимосвязи между аудиторной и самостоятельной работой студентов, для чего в рамках курса предлагается набор активных и интерактивных методов занятий в развитие сюжетов, рассмотренных в рамках лекций и практических занятий.

Методические указания по теме 1

При подготовке к занятиям по теме «Теоретические основы информационной безопасности» студенту необходимо обратиться к конспектам лекции 1 и книге Анисимова А.А. «Менеджмент в сфере информационной безопасности» (основная литература, источник 1).

Контроль самостоятельной работы проводится в форме индивидуального консультирования в целях дополнительного разъяснения обучающимся вопросов, связанных с классификацией угроз безопасности и надежностью безопасности.

Формой текущего контроля успеваемости по теме «Теоретические основы

информационной безопасности» является устный опрос. Выбранная форма контроля способствует формированию навыка краткого и систематичного устного изложения изученного материала.

Шкала оценивания для устного опроса

Оценка	Требования к знаниям
«зачтено»	Оценка «зачтено» выставляется, если студентом: <ol style="list-style-type: none"> 1. продемонстрировано отличное знание изученного материала и владение категориальным аппаратом 2. дан правильный ответ на вопрос с использованием профессиональной лексики и терминологии
«не зачтено»	Оценка «не зачтено» выставляется студенту, если студентом содержание темы раскрыто фрагментарно и имеются существенные пробелы в знаниях категориального аппарата

Методические указания по теме 2

При подготовке к занятиям по теме «Обеспечение информационной безопасности в условиях глобализации информационного пространства» студенту необходимо обратиться к конспектам лекции 2 и книге Анисимова А.А. «Менеджмент в сфере информационной безопасности» (основная литература, источник 1).

Контроль самостоятельной работы проводится в форме индивидуального консультирования в целях дополнительного разъяснения обучающимся вопросов, связанных с правовыми средствами обеспечения информационной безопасности.

Формой текущего контроля успеваемости по теме «Обеспечение информационной безопасности в условиях глобализации информационного пространства» является разбор кейса.

Шкала оценивания для кейса

Оценка	Требования к знаниям
«зачтено»	Оценка «зачтено» выставляется, если студентом: <ol style="list-style-type: none"> 1. продемонстрировано владение навыком анализа бизнес-ситуаций с использованием изученных инструментов 2. дана развернутые ответы к кейсу и обоснована собственная точка зрения с использованием иллюстрирующих примеров из теста кейса или собственного опыта
«не зачтено»	Оценка «не зачтено» выставляется студенту, если студентом задание выполнено не в полном объеме

Методические указания по теме 3

При подготовке к занятиям по теме «Правовые режимы обеспечения безопасности информации ограниченного доступа» студенту необходимо обратиться к конспектам лекции 3 и книге Галатенко В.А. «Основы информационной безопасности» (основная литература, источник 2).

Контроль самостоятельной работы проводится в форме индивидуального консультирования в целях дополнительного разъяснения обучающимся вопросов, связанных с особенностями обеспечения безопасности информации ограниченного доступа.

Формой текущего контроля успеваемости по теме «Правовые режимы обеспечения безопасности информации ограниченного доступа» является письменный опрос. Выбранная форма контроля способствует формированию навыка краткого и систематичного изложения изученного материала.

Шкала оценивания для опроса

Оценка	Требования к знаниям
«зачтено»	Оценка «зачтено» выставляется, если студентом: <ol style="list-style-type: none"> 1. продемонстрировано отличное знание изученного материала и владение категориальным аппаратом 2. дан правильный ответ на вопрос с использованием профессиональной лексики и терминологии
«не зачтено»	Оценка «не зачтено» выставляется студенту, если студентом содержание темы раскрыто фрагментарно и имеются существенные пробелы в знаниях категориального аппарата

Методические указания по теме 4

При подготовке к занятиям по теме «Юридическая ответственность за правонарушения в информационной сфере» студенту необходимо обратиться к конспектам лекции 4 и книге Галатенко В.А. «Основы информационной безопасности» (основная литература, источник 2).

Контроль самостоятельной работы проводится в форме индивидуального консультирования в целях дополнительного разъяснения обучающимся вопросов, связанных с особенностями юридической ответственности в информационной сфере.

Формой текущего контроля по теме «Юридическая ответственность за правонарушения в информационной сфере» является написание эссе. Эссе выполняется по одной из предложенных тем. Объем готовой работы не должен превышать 1500 знаков. На выполнение работы студентам отводится 1 неделя.

Шкала оценивания для эссе

Оценка	Требования к знаниям
«зачтено»	Оценка «зачтено» выставляется, если студентом: <ol style="list-style-type: none"> 1. сделана обоснованная оценка взглядов других людей, особенно противоречащих его собственным 2. четко высказана собственная позиция по данному вопросу 3. приведены доводы, четко связанные друг с другом и расположенные в логическом порядке 4. использованы исследования других людей для поддержания доказательства и усиления аргументации
«не зачтено»	Оценка «не зачтено» выставляется студенту, если студентом <ol style="list-style-type: none"> 1. не сделана обоснованная оценка взглядов других людей, особенно противоречащих его собственным 2. не высказано собственная позиция по данному вопросу 3. приведены доводы, четко не связанные друг с другом 4. не использованы исследования других людей для поддержания доказательства и усиления аргументации

Методические указания по теме 5

При подготовке к занятиям по теме «Проектирование систем защиты информации» студенту необходимо обратиться к конспектам лекции 5 и книге Аверченкова В.И. «Аудит информационной безопасности» (основная литература, источник 3).

Контроль самостоятельной работы проводится в форме индивидуального консультирования в целях дополнительного разъяснения обучающимся вопросов, связанных с проектированием моделей систем защиты информации.

Формой текущего контроля по теме «Проектирование систем защиты информации»

является тестирование. Тестирование студентов проводится в аудитории под контролем преподавателя. На выполнение одного варианта теста, состоящего из 30 вопросов, студентам отводится 60 минут. В зависимости от уточнения в вопросе, правильных ответов может быть от 1 до 4.

Шкала оценивания для тестирования

Оценка	Требования к знаниям
«зачтено»	Оценка «зачтено» выставляется, если студентом даны верные ответы на 70% и более вопросов
«не зачтено»	Оценка «не зачтено» выставляется студенту, если студентом даны верные ответы менее, чем на 70% вопросов

Методические указания по теме 6

При подготовке к занятиям по теме «Анализ и управление рисками в сфере информационной безопасности» студенту необходимо обратиться к конспектам лекции 6 и книге Аверченко В.И. «Аудит информационной безопасности» (основная литература, источник 3).

Контроль самостоятельной работы проводится в форме индивидуального консультирования в целях дополнительного разъяснения обучающимся вопросов, связанных с особенностями анализа и управления информационной безопасностью.

Формой текущего контроля по теме «Анализ и управление рисками в сфере информационной безопасности» является тестирование. Тестирование студентов проводится в аудитории под контролем преподавателя. На выполнение одного варианта теста, состоящего из 30 вопросов, студентам отводится 60 минут. В зависимости от уточнения в вопросе, правильных ответов может быть от 1 до 4.

Шкала оценивания для тестирования

Оценка	Требования к знаниям
«зачтено»	Оценка «зачтено» выставляется, если студентом даны верные ответы на 70% и более вопросов
«не зачтено»	Оценка «не зачтено» выставляется студенту, если студентом даны верные ответы менее, чем на 70% вопросов

Подготовка к промежуточной аттестации:

На первом занятии преподаватель информирует обучающихся о применяемой системе текущего контроля успеваемости и форме промежуточной аттестации.

Во время последующих аудиторных занятий – доводит до студентов информацию о результатах текущего контроля успеваемости.

К промежуточной аттестации необходимо готовится целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. Попытки освоить дисциплину в период зачётно-экзаменационной сессии, как правило, показывают не удовлетворительные результаты. В самом начале изучения учебной дисциплины познакомьтесь со следующей учебно-методической документацией:

- программой дисциплины;
- перечнем знаний и умений, которыми студент должен владеть;
- тематическими планами лекций, семинарских занятий;
- контрольными мероприятиями;
- учебником, учебными пособиями по дисциплине, а также
- электронными ресурсами;
- перечнем вопросов к зачету

После этого у вас должно сформироваться четкое представление об объеме и характере получаемых знаний и умений по дисциплине. Систематическое выполнение учебной работы на лекциях и практических занятиях позволит успешно освоить дисциплину и создать хорошую базу для сдачи зачета

При подготовке к промежуточной аттестации студентам рекомендуется проработать следующие вопросы:

1. Цели государства в области обеспечения информационной безопасности.
2. Основные нормативные акты РФ, связанные с правовой защитой информации.
3. Виды компьютерных преступлений.
4. Способы и механизмы совершения информационных компьютерных преступлений.
5. Основные параметры и черты информационной компьютерной преступности в России.
6. Компьютерный вирус. Основные виды компьютерных вирусов.
7. Методы защиты от компьютерных вирусов.
8. Типы антивирусных программ.
9. Защиты от несанкционированного доступа. Идентификация и аутентификация пользователя.
10. Основные угрозы компьютерной безопасности при работе в сети Интернет.
11. Виды защищаемой информации.
12. Государственная тайна как особый вид защищаемой информации.
13. Конфиденциальная информация.
14. Система защиты государственной тайны.
15. Правовой режим защиты государственной тайны.
16. Защита интеллектуальной собственности средствами патентного и авторского права.
17. Международное законодательство в области защиты информации.
18. Программно-аппаратные средства обеспечения информационной безопасности в информационных сетях.
19. Симметричные шифры.
20. Ассиметричные шифры.
21. Место и роль теории организации в системе управленческих знаний. Предмет и методы теории организации. Общее понятие организации. Понятие системы и свойства систем
22. Понятие поведения, адаптации и устойчивости системы. Критерии эффективности организационных систем
23. Характеристики организации как социально-экономической системы. Понятие социальной организации, её характеристика
24. Внешняя среда социально-экономической системы. Внутренняя среда организации. Влияние среды на функционирование производственной организации: этап массового производства, этап массового сбыта, постиндустриальный этап.
25. Понятие организационной структуры управления, взаимосвязь целей, функций и структуры. Требования к организационной структуре управления. Принципы построения организационной структуры управления.
26. Решения в процессе управления. Требования, предъявляемые к управленческим решениям. Классификация управленческих решений. Схема процесса подготовки, разработки, принятия и реализации управленческих решений. Факторы, влияющие на эффективность и качество управленческих решений.

**6. Учебная литература и ресурсы информационно-телекоммуникационной сети
"Интернет", учебно-методическое обеспечение самостоятельной работы
обучающихся по дисциплине**

6.1. Основная литература

1. Анисимов А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс] / А.А. Анисимов. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 212 с. — 978-5-9963-0237-6. — Режим доступа: <http://www.iprbookshop.ru/52182.html>
2. Галатенко В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 266 с. — 978-5-94774-821-5. — Режим доступа: <http://www.iprbookshop.ru/52209.html>
3. Аверченков В.И. Аудит информационной безопасности [Электронный ресурс] : учебное пособие для вузов / В.И. Аверченков. — Электрон. текстовые данные. — Брянск: Брянский государственный технический университет, 2012. — 268 с. — 978-89838-487-6. — Режим доступа: <http://www.iprbookshop.ru/6991.html>

6.2. Дополнительная литература

1. Махов С.Ю. Аналитика безопасности [Электронный ресурс] : учебное пособие / С.Ю. Махов. — Электрон. текстовые данные. — Орел: Межрегиональная Академия безопасности и выживания (МАБИБ), 2013. — 239 с. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/33422.html>
2. Гуманитарные аспекты информационной безопасности [Электронный ресурс] : методология и методика поиска истины, построения доказательств и защиты от манипуляций / Э.П. Теплов [и др.]. — Электрон. текстовые данные. — СПб. : Университет ИТМО, 2016. — 123 с. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/66436.html>
3. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под ред. Т. А. Поляковой, А. А. Стрельцова. — М. : Издательство Юрайт, 2017. — 325 с
4. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — М. : Издательство Юрайт, 2017. — 321 с.
5. Внуков, А. А. Защита информации : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2017. — 261 с
6. Тихонов В.А., Райх В.В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: уч. пособие. —М.: Гелиос АРВ, 2006.— 528 с.
7. Пичугин В.Г. Безопасность бизнеса: Защита от уголовного преследования. — М:
8. Альпина Паблишерз, 2010. — 174 с.
9. Гаврилов Л.П. Основы электронной коммерции и бизнеса: Учебное пособие. Солон-Пресс, 2009. — 592 с.

6.3. Учебно-методическое обеспечение самостоятельной работы

1. Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование : учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. — М. : Издательство Юрайт, 2017. — 220 с.
2. Государственная тайна и ее защита в Российской Федерации: Учебное пособие // под общ.ред. М.А.Вуса и А.В.Федорова С-Пб.2007

6.4. Нормативные правовые документы

1. Стратегия развития информационного общества в Российской Федерации" (утв. Президентом РФ 07.02.2008 N Пр-212)
2. Федеральный закон «Об информации, информационных технологиях и о защите информации № 149-ФЗ от 27 июля 2006 года
3. Федеральный закон от 23.08.1996 N 127-ФЗ «О науке и государственной научно-технической политике» // СЗ РФ 26.08.1996, N 35, ст. 4137
4. Распоряжение Правительства РФ от 17.11.2008 N 1662-р « О Концепции долгосрочного социально-экономического развития Российской Федерации на период до 2020 года» // СЗ РФ 24.11.2008, N 47, ст. 5489.
5. Указ Президента РФ от 01.11.2008 № 1576 «О Совете при Президенте Российской Федерации по развитию информационного общества в Российской Федерации»
6. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных»
7. Федеральный закон от 19.12.2005 N 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»
8. Федеральный закон от 19.12.2005 N 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»

6.5. Интернет-ресурсы

1. www.nnir.ru / - Российская национальная библиотека
2. www.nns.ru / - Национальная электронная библиотека
3. www.rsi.ru / - Российская государственная библиотека
4. www.biznes-karta.ru / - Агентство деловой информации «Бизнес-карта»
5. www.rbs.ru / - Информационное агентство «РосБизнесКонсалтинг»
6. www.google.com / - Поисковая система
7. www.rambler.ru / - Поисковая система
8. www.yandex.ru / - Поисковая система
9. www.busineslearning.ru / - Система дистанционного бизнес образования
10. <http://www.consultant.ru/> - Консультант плюс
11. <http://www.garant.ru/> - Гарант
12. www.economist.com/ - журнал The Economist
13. www.ft.com / - газета The Financial Times
14. www.forbes.com/management / - Новости бизнеса (менеджмент)
15. www.management.about.com / - Управление и лидерство
16. www.rbc.ru / - Деловые новости
17. www.kommersant.ru / - газета Коммерсантъ
18. www.vedomosti.ru / - газета Ведомости

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

Специальные помещения представляют собой учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Помещения укомплектованы специализированной мебелью и техническими средствами обучения.

Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации, соответствующие рабочим учебным программам дисциплин.

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к нескольким электронно-библиотечным системам (электронным библиотекам) и к электронной информационно-образовательной среде организации. Электронно-библиотечная система (электронная библиотека) и электронная информационно-образовательная среда обеспечивают возможность доступа обучающегося из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет», как на территории организации, так и вне ее.

Академия обеспечена необходимым комплектом лицензионного программного обеспечения.

Обучающимся обеспечен доступ (удаленный доступ), в том числе в случае применения электронного обучения, дистанционных образовательных технологий, к современным профессиональным базам данных и информационным справочным системам.

Организован доступ к следующим электронным ресурсам:

- [Bloomberg](#)
- [EBSCO Publishing](#)
- [eLIBRARY.RU](#)
- [Emerging Markets Information Service](#)
- [Google Scholar \(Google Академия\)](#)
- [IMF eLibrary](#)
- [JSTOR](#)
- [New Palgrave Dictionary of Economics - Электронный словарь.](#)
- [OECD iLibrary](#)
- [Oxford Handbooks Online](#)
- [Polpred.com Обзор СМИ](#)
- [Science Direct - Журналы издательства Elsevier по экономике и эконометрике, бизнесу и финансам, социальным наукам и психологии, математике и информатике; SCOPUS](#)
- [Web of Science](#)
- [Wiley Online Library](#)
- [World Bank Elibrary](#)
- [Архивы научных журналов NEICON](#)
- [Интернет-сервис «Антиплагиат»](#)
- [Система Профессионального Анализа Рынков и Компаний «СПАРК»](#)
- [ЭБС Издательства "Лань"](#)
- [ЭБС Юрайт](#)
- [Электронная библиотека Издательского дома «Гребенников»](#)