Федеральное государственное автономное образовательное учреждение высшего образования «Российский университет дружбы народов»

Институт мировой экономики и бизнеса

Рекомендовано
МССН/МО

1. РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Рекомендуется для направления подготовки/специальности 38.03.01 «Экономика»

(указываются код и наименование направления подготовки/специальности)

Направленность программы (профиль) «Международная экономическая безопасность»

(наименование образовательной программы в соответствии с направленностью (профилем)

Раздел I. Основная часть

1. 1. Учебная программа дисциплины «Информационная безопасность»

1.1. Содержание дисциплины:

Основной целью освоения учебной дисциплины «Информационная безопасность» является ознакомление студентов с основными направлениями деятельности по обеспечению информационной безопасности и защите информации, рассмотрение аспектов нормативно-правовой базы, регламентирующей данную деятельность, задач руководителей, специалистов по сохранности информационных ресурсов, средств и механизмов, в том числе аппаратно-программных, используемых для этих целей, и, конечно, методов их применения.

Необходимость (актуальность) изучения учебной дисциплины в рамках бакалавриат экономики по направлению подготовки специалистов по специальности 38.03.01 Международная экономическая безопасность обусловлена тем, что в современных условиях динамично изменяющегося мира и нарастания угроз экономической безопасности Российской Федерации. Продолжающийся мировой экономический кризис и политическая нестабильность, несовершенство законодательной базы, секторальные санкции введенные странами Запада против Российской Федерации, в нарушение основополагающих принципов ВТО. В этих сложных условиях органам государственной власти приходится решать все более сложные задачи в этой области. Для их решения необходимы профессиональные знания и умения анализировать угрозы экономическим интересам страны, вырабатывать предложения по их нейтрализации, перераспределять ресурсы, силы и средства.

Задачи изучения дисциплины «Информационная безопасность»:

- сформировать общее представление об информационной безопасности как о состоянии защищенности информационного ресурса сложной системы, понимание необходимости системного подхода к практической реализации такого состояния;
- передать знания о порядке организации и практической реализации типовых мероприятий по обеспечению информационной безопасности и защите информации;
- сформировать навыки анализа информационных ресурсов по следующим факторам: важность, конфиденциальность, уязвимость.

Курс преследует несколько важнейших целей. В частности, освоив курс, студент должен получить возможность:

- во-первых, приобрести высокий уровень компетенций в области информационной безопасности для работы в государственных и частно-государственных структурах в том числе и с целью повышения эффективности их деятельности.
- во-вторых, стать руководителем или специалистом государственного или муниципального управления.
- в-третьих, применить свои силы в сфере регионального и муниципального управления.

Место дисциплины в структуре ОП ВО:

Дисциплина «Информационная безопасность» относится к вариативной части учебного плана.

В таблице № 1 приведены предшествующие и последующие дисциплины, направленные на формирование компетенций дисциплины в соответствии с матрицей компетенций ОП ВО.

Таблица № 1

Предшествующие и последующие дисциплины, направленные на формирование компетенций

№ п/п	Шифр и наименование компетенции	Предшествующие дисциплины	Последующие дисциплины (группы дисциплин)
Универсальные компетенции			
	УК-12 - Способен к взаимодействию в условиях современной информационной культуры и цифровой экономики с учетом требований информационной безопасности, этических и правовых норм	Основы безопасности государства Правовое обеспечение экономической безопасности	Финансовая безопасность, Глобальная и региональная безопасность
Общепрофессиональные компетенции			
	ОПК-2 - Способен осуществлять сбор, обработку и статистический анализ данных, необходимых для решения поставленных экономических задач; ОПК-5 - Способен использовать современные информационные технологии и программные средства при решении профессиональных задач.		
Профессиональные компетенции (вид профессиональной деятельности)			
	ПК – 1 - способность анализировать и интерпретировать данные отечественной и зарубежной статистики о социально-экономических процессах и явлениях, выявлять тенденции изменения социально-экономических показателей	Экономическая информатика Основы безопасности государства Правовое обеспечение экономической безопасности	Банковское дело Финансовая безопасность Информационные системы в экономике

Требования к результатам освоения дисциплины:

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- Способность к взаимодействию в условиях современной информационной культуры и цифровой экономики с учетом требований информационной безопасности, этических и правовых норм (УК-12);

- Способность осуществлять сбор, обработку и статистический анализ данных, необходимых для решения поставленных экономических задач (ОПК-2);

- Способен использовать современные информационные технологии и программные средства при решении профессиональных задач. (ОПК-5);

- Способность анализировать и интерпретировать данные отечественной и зарубежной статистики о социально-экономических процессах и явлениях, выявлять тенденции изменения социально-экономических показателей (ПК-1).

В результате изучения дисциплины студент должен:

Знать:

основы теории информационной безопасности: внешние и внутренние угрозы интересам в информационной сфере; сущность внешне- и внутриэкономической безопасности, других видов экономической безопасности, основы их обеспечения; нормативно-правовые документы, применяемые в профессиональной деятельности, систему категорий и методов, направленных на формирование аналитического и логического мышления; основные математические и статистические методы обработки данных, полученных при решении основных профессиональных задач, основы библиографической и информационно-поисковой работы.

Уметь:

выявлять современные проблемы информационной безопасности Российской Федерации и ее регионов, определять основные направления их разрешения; оценивать и проводить мониторинг эффективности обеспечения информационной безопасности страны и ее регионов; использовать нормативно-правовые документы в практической деятельности, анализировать и оценивать профессиональную информацию, обобщать, строить выводы, использовать данные поисковой системы при решении профессиональных задач и оформлении научных статей, отчетов, заключений и пр.

Владеть:

навыками самостоятельной работы, самоорганизации и организации выполнения поручений; основными методами защиты интересов в информационной сфере; навыками выявления, анализа и оценки угроз этим интересам; навыками работы в составе органов управления по нейтрализации угроз; навыками работы с нормативно-правовыми документами. навыками управления информацией, составления и оформления отчетов, заключений и т.д.; навыками решения типовых задач в различных областях профессиональной практики (навыками анализа своей деятельности с целью ее оптимизации, навыками использования в профессиональной деятельности базовых знаний информатики и современных информационных технологий.

Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет _____2_____ зачетных единицы.

Вид учебной работы	Всего часов	Семестры			
		5			
Аудиторные занятия (всего)	36	36			
В том числе:	-	-			
Лекции	18	18			
Практические занятия (ПЗ)	-	-			
Семинары (С)	18	18			
Лабораторные работы (ЛР)	-	-			

Самостоятельная работа (всего)	36	36			
Общая трудоемкость час зач. ед.	72	72			
	2				

1.2. Содержание дисциплины

Содержание разделов дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела (темы)
1	Современное состояние и правовое регулирование сферы информационной безопасности.	Понятие информационной безопасности. Цели обеспечения информационной безопасности. Основные задачи, решаемые при обеспечении информационной безопасности. Законодательные основы по защите информации (Федеральный закон "Об информации, информатизации и защите информации", Закон "О коммерческой тайне", Закон "О банках и банковской деятельности в РФ"и др.). Цели защиты информации. Атака на информацию. Экономические и моральные последствия атаки на информацию. Пять уровней обеспечения информационной безопасности (системы защиты): Законодательный, Морально-этический, Административный, Физический, Аппаратно-программный. Основные принципы выстраивания надежной системы защиты. Законодательство Российской Федерации и иностранных государств в области информационной безопасности. Конституционные гарантии прав граждан на информацию и механизм их реализации. Понятие и виды защищаемой информации по законодательству Российской Федерации. Понятие государственной, коммерческой, личной тайны. Основные нормативные документы в этой области. Рассекречивание документов. Уровень тайны. Международное законодательство в области защиты информации. Стандарты в области информационной безопасности. Международные стандарты информационного обмена.
2	Угрозы информационной безопасности и методы их реализации.	Модели оценки ценности информации. Классификация и общий анализ угроз безопасности информации. Причины, виды, каналы утечки и искажения информации. Основные методы реализации угроз информационной безопасности: методы нарушения конфиденциальности, целостности и доступности информации. Модель нарушителя. Угрозы секретности (конфиденциальности) информации: разглашение, утечка, несанкционированный доступ. Информационная безопасность в условиях функционирования глобальных сетей. Понятие компьютерного вируса. История появления компьютерных вирусов и факторы, влияющие на их распространение. Вирусы как класс вредоносного

		программного обеспечения. Классификация компьютерных вирусов. Компьютерная преступность. Классификация компьютерных преступлений. Понятие нарушителя информационной безопасности. Хакеры. Виды хакеров. Примеры хакерских атак.
3	Место информационной безопасности экономических систем в национальной безопасности страны.	Схема построения информационной безопасности на уровне государства. Информационная безопасность страны. Защита экономических систем. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации. Национальные интересы Российской Федерации в информационной сфере и их обеспечение. Интересы личности в информационной сфере. Интересы общества в информационной сфере. Интересы государства в информационной сфере. Основные составляющие национальных интересов Российской Федерации в информационной сфере. Виды угроз информационной безопасности Российской Федерации. Источники угроз информационной безопасности Российской Федерации. Внешние источники угроз. Внутренние источники угроз. Направления обеспечения информационной безопасности государства. Проблемы региональной информационной безопасности Основные положения государственной политики обеспечения информационной безопасности иностранных государств. Доктрина информационной безопасности Российской Федерации. Система обеспечения информационной безопасности. Особенности обеспечения информационной безопасности в правоохранительных органах.
4	Способы и средства обеспечения защиты информации.	Сущность и перечень организационных мер по защите информации. Субъекты деятельности по защите информации. Структура и задачи подразделения по защите информации. Сущность и перечень инженерно-технических мер по защите информации. Методика и средства защиты информации. Средства контроля эффективности защиты информации. Средства физической защиты информации. Классификация программных средств защиты информации. Использование программ для обеспечения безопасности конфиденциальной информации. Технологии защиты программного обеспечения. Защита информации от утечки, несанкционированного доступа и несанкционированного воздействия. Защита информации от непреднамеренного воздействия, разглашения и разведки. Аудит информационной безопасности. Управление рисками.

5	Информационная безопасность автоматизированных систем.	Проблемы обеспечения безопасности обработки и хранения информации в вычислительных системах. Базовые этапы построения системы комплексной защиты вычислительных систем. Угрозы информационно-программному обеспечению вычислительных систем и их классификация. Классификация методов защиты информации с использованием программно-аппаратных средств вычислительной системы. Организационная структура системы комплексной защиты информационно-программного обеспечения. Общие сведения о реализации защиты информационно-программного обеспечения в операционных системах. Подходы к построению защищенной операционной системы. Административные меры защиты. Виды уязвимости и атак на операционные системы. Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам. Основные этапы допуска к ресурсам вычислительной системы. Использование простого и динамически изменяющегося паролей. Способы разграничения доступа к компьютерным ресурсам. Защита программных средств от несанкционированного копирования, исследования и модификации. Защита офисных документов. Привязка программ к среде функционирования. Защита программ от несанкционированного запуска. Общая организация защиты от компьютерных вирусов. Защита от деструктивных действий и размножения вирусов. Использование средств аппаратного и программного контроля. Технология гарантированного восстановление вычислительной системы после заражения компьютерными вирусами. Программные средства обслуживания операционных систем. Утилиты и специализированные программы профилактики компьютера. Программные средства восстановления информации. Защита электронных запоминающих устройств.
6	Безопасность компьютерных сетей.	Компьютерные сети, топология сетей, структура Интернет. Принципы передачи информации в сети (протокол TCP/IP, доменная система имен, пакеты, порты, сетевые службы). Принципы работы традиционных механизмов защиты компьютерных сетей. Организация защиты от несанкционированного доступа. Защита Интернет-подключений. Функции межсетевых экранов, понятие брандмауэра. Технологии межсетевых экранов (фильтрация пакетов, применение шлюзов, прочие компоненты брандмауэров (файрволлов). Брандмауэр Windows, настройка и определение правил.

		Журналы доступа. Выявление следов несанкционированного доступа к файлам. Сканеры и автоматизация поиска слабых мест в защите сети и в защите системы. Анализаторы протоколов. Возможности выявления и раскрытия преступлений в сфере компьютерной информации и высоких технологий. Противодействие распространению наркотиков в сети Интернет.
7	Криптографическая защита информации.	Криптография, Криптоанализ. Основные понятия криптологии. История шифрования. Использование шифрования различными методами. Симметричные и несимметричные системы шифрования информации. Рассмотрение сокрытия информации таблицей Винжера. Программы для криптографии. Криптографические алгоритмы. Электронная цифровая подпись (ЭЦП) и функция хэширования. Создание и использование криптоключей. Подтверждение подлинности объектов и субъектов информационной системы. Понятие криптографической стойкости, вопросы практической стойкости. Программно-аппаратные средства криптозащиты данных.

(Содержание указывается в дидактических единицах. По усмотрению разработчиков материал может излагаться не в форме таблицы).

Разделы дисциплин и виды занятий

№ п/п	**Наименование раздела дисциплины**	**Лекц.**	**Практ. Зан.**	**Лаб. Зан.**	**Семин**	**СРС**	**Все-го час.**
Второй семестр							
1	Современное состояние и правовое регулирование сферы информационной безопасности.	2	-	-	2	4	8
2	Место информационной безопасности экономических систем в национальной безопасности страны.	2	-	-	2	4	8
3	Угрозы информационной безопасности и методы их реализации.	2	-	-	2	8	12
4	Способы и средства обеспечения защиты информации.	2	-	-	2	4	14
5	Информационная безопасность автоматизированных систем.	2	-	-	2	6	10
6	Безопасность компьютерных сетей.	3	-	-	3	6	12
7	Криптографическая защита информации.	4	-	-	4	6	14
ИТОГО		17	-	-	17	38	72

Лабораторный практикум – не предусмотрен
Практические занятия – не предусмотрены

1.3. Перечень основной и дополнительной учебной литературы

Основная литература:

1. Внуков А. А. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ЗАЩИТА ИНФОРМАЦИИ – М.: Издательство Юрайт, 2019. – 240 с. /ЭБС Book.ru [Электронный ресурс]. - URL: https://biblio-online.ru/book/osnovy-informacionnoy-bezopasnosti-zaschita-informacii-431332
2. Нестеров С. А. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. – М.: Издательство Юрайт, 2019. – 321 с. /ЭБС Book.ru [Электронный ресурс]. - URL: https://biblio-online.ru/book/informacionnaya-bezopasnost-442312
3. Полякова Т. А., Стрельцов А. А., Чубукова С. Г., Ниесов В. А. ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. – М.: Издательство Юрайт, 2019. – 325 с. /ЭБС Book.ru [Электронный ресурс]. - URL: https://biblio-online.ru/book/organizacionnoe-i-pravovoe-obespechenie-informacionnoy-bezopasnosti-432966
4. Щеглов А. Ю., Щеглов К. А. ЗАЩИТА ИНФОРМАЦИИ: ОСНОВЫ ТЕОРИИ. – М.: Издательство Юрайт, 2019. – 309 с. /ЭБС Book.ru [Электронный ресурс]. - URL:https://biblio-online.ru/book/zaschita-informacii-osnovy-teorii-433715

Дополнительная литература:

1. Васильков А.В. Безопасность и управление доступом в информационных системах: учебное пособие / Васильков А.В., Васильков И.А. - М.:Форум, НИЦ ИНФРА-М, 2017. - 368 с.
2. Казарин О. В., Забабурин А. С. Программно-аппаратные средства защиты информации. Защита программного обеспечения– М.: Издательство Юрайт, 2019. — 312 с. —. ЭБС Book.ru [Электронный ресурс]. - URL: https://biblio-online.ru/book/programmno-apparatnye-sredstva-zaschity-informacii-zaschita-programmnogo-obespecheniya-437163
3. Мельников, А.И. Куприянов, Т.Ю. Васильева Информационная безопасность: — М. Издательство РУСАЙНС, 2016. —354 с. —. /ЭБС Book.ru [Электронный ресурс]. - URL:https://www.book.ru/book/920736/view2/1

Нормативные правовые документы

Приводятся дата принятия и номер нормативного правового акта в первой редакции. При подготовке к занятиям необходимо использовать последние редакции указанных документов, которые находятся в справочных правовых системах КонсультантПлюс, ГАРАНТ или специальной библиотеке.

1. Конституция Российской Федерации : принята всенародным голосованием 12.12.1993.
2. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ.
3. О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ.
4. О коммерческой тайне : Федеральный закон от 29.07.2004 № 98-ФЗ.
5. О связи : Федеральный закон от 07.07.2003 № 126-ФЗ.
6. Об электронной подписи : Федеральный закон от 06.04.2011 № 63-ФЗ.
7. О лицензировании отдельных видов деятельности : Федеральный закон от 04.05.2011 № 99-ФЗ.
8. О государственной тайне : закон РФ от 21.07.1993 № 5485-1.
9. Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента РФ от 05.12.2016 № 646.

10. Об утверждении Перечня сведений, отнесенных к государственной тайне : Указ Президента РФ от 30.11.1995 № 1203.
11. Об утверждении Перечня сведений конфиденциального характера : Указ Президента РФ от 06.03.1997 № 188.
12. О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно- телекоммуникационных сетей международного информационного обмена : Указ Президента РФ от 17.03.2008 № 351.
13. Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти : постановление Правительства РФ от 03.11.1994 № 1233.
14. О сертификации средств защиты информации : постановление Правительства РФ от 26.06.1995 № 608.
15. Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности : постановление Правительства РФ от 04.09.1995 № 870.
16. Государственная программа Российской Федерации «Информационное общество (2011–2020 годы)» : распоряжение Правительства РФ от 15.04.2014 № 313.
17. Положение о сертификации средств защиты информации по требованиям безопасности информации : приказ Гостехкомиссии РФ от 27.10.1995 № 199.
18. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : приказ ФСТЭК России от 11.02.2013 № 17.
19. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : приказ ФСТЭК России от 18.02.2013 № 21.
20. ГОСТ Р 52292-2004. Информационная технология. Электронный обмен информацией. Термины и определения : утвержден приказом Ростехрегулирования от 29.12.2004 № 135-ст.
21. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения : утвержден приказом Ростехрегулирования от 27.12.2006 № 373-ст.
22. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения : утвержден приказом Ростехрегулирования от 27.12.2006 № 374-ст.

Информационные ресурсы

1. Университетская информационная система РОССИЯ [Электронный ресурс] URL:https://uisrussia.msu.ru/
2. Федеральная служба государственной статистики [Электронный ресурс] URL:http://www.gks.ru/
3. портал Электронная библиотека: диссертации [Электронный ресурс] URL:http://diss.rsl.ru/?menu=disscatalog/
4. Сайт Министерства экономического развития Российской Федерации [Электронный ресурс] URL:http://economy.gov.ru/minec/main
5. Сайт Министерства финансов Российской Федерации [Электронный ресурс] URL:https://m.minfin.ru/ru/
6. Сайт Министерства промышленности и торговли Российской Федерации [Электронный ресурс] URL:http://minpromtorg.gov.ru/
7. Сайт Министерства труда и социальной защиты Российской Федерации [Электронный ресурс] URL:https://rosmintrud.ru/
8. Сайт Министерства природных ресурсов и экологии Российской Федерации [Электронный ресурс] URL:http://www.mnr.gov.ru/

9. Сайт Федеральной службы по финансовому мониторингу [Электронный ресурс] URL:http://www.fedsfm.ru/
10. Сайт Федеральной антимонопольной службы [Электронный ресурс] URL:https://fas.gov.ru/
11. Сайт Федеральной службы государственной статистики [Электронный ресурс] URL:http://www.gks.ru/

1.4. Описание материально-технической базы (материально-техническое оснащение дисциплины)

1	ФРЦ1 Рабочее место: сист блок P4 C2D /2550 MHz/2048 MB/ 250GB/DVD±RW/ LCDmonitor 17" Microsoft Office 2007 ProjectExpert 7 Tutorial	Миклухо-Маклая, 6, библиотека, ФРЦ, ком.1
2.	ФРЦ3 Рабочее место: сист блок P4 C2D /2550 MHz/2048 MB/ 250 GB/DVD±RW/ LCD monitor 17"/проектор Microsoft Office 2007	Миклухо-Маклая, 6, библиотека, ФРЦ, ком.3
3.	101 Мультимедиа проектор – 2 шт., звуковая трибуна – 1 шт., экран -2 шт.	Миклухо-Маклая, 6, ком.101
4	107 Мультимедиа проектор – 1 шт., экран -1 шт.	Миклухо-Маклая, 6, ком.107
5.	109 Мультимедиа проектор – 1 шт., оборудование конференц-связи, DVD- рекордер, звуковое оборудование, экран – 1 шт.	Миклухо-Маклая, 6, ком.109
6.	17 Мультимедиа проектор – 2 шт., звуковая трибуна – 1 шт., экран – 2 шт.	Миклухо-Маклая, 6, ком.17
7	27 Мультимедиа проектор – 1 шт., экран – 1 шт.	Миклухо-Маклая, 6, ком.27
8.	Конференц.зал ЭФ Мультимедиа проектор – 1 шт., звуковое оборудование	Миклухо-Маклая, 6, Конференц. зал ЭФ

1.5. Учебники

1. Внуков А. А. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ЗАЩИТА ИНФОРМАЦИИ – М.: Издательство Юрайт, 2019. – 240 с. /ЭБС Book.ru [Электронный ресурс]. - URL: https://biblio-online.ru/book/osnovy-informacionnoy-bezopasnosti-zaschita-informacii-431332
2. Нестеров С. А. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. – М.: Издательство Юрайт, 2019. – 321 с. /ЭБС Book.ru [Электронный ресурс]. - URL: https://biblio-online.ru/book/informacionnaya-bezopasnost-442312
3. Полякова Т. А., Стрельцов А. А., Чубукова С. Г., Ниесов В. А. ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. – М.: Издательство Юрайт, 2019. – 325 с. /ЭБС Book.ru [Электронный ресурс]. - URL: https://biblio-online.ru/book/organizacionnoe-i-pravovoe-obespechenie-informacionnoy-bezopasnosti-432966

4. Щеглов А. Ю., Щеглов К. А. ЗАЩИТА ИНФОРМАЦИИ: ОСНОВЫ ТЕОРИИ. – М.: Издательство Юрайт, 2019. – 309 с. /ЭБС Book.ru [Электронный ресурс]. - URL:https://biblio-online.ru/book/zaschita-informacii-osnovy-teorii-433715

1.6. Перечень информационных технологий

программное обеспечение

Windows, MSOffice (MSWord, MSExcel, PowerPointит.п.), Internet.

базы данных, информационно-справочные и поисковые системы

- Электронный каталог – база книг и периодики в фонде библиотеки РУДН.
- Электронные ресурсы – в том числе раздел - Лицензированные ресурсы

УНИБЦ (НБ):

1. Университетская библиотека ONLINE
2. SPRINGER. Книжные коллекции издательства
3. Вестник РУДН
4. EastView

Универсальные базы данных:

1. eLibrary.ru
2. Grebennikon
3. Электронная библиотека диссертаций РГБ
4. Справочно-правовая система «Консультант Плюс».
5. Информационно-правовое обеспечение «Гарант».

Раздел II. Самостоятельная работа студента.

2.1. Перечень домашних заданий по темам

Тема 1.

1. Основные задачи, решаемые при обеспечении информационной безопасности.
2. Законодательные основы по защите информации (Федеральный закон "Об информации, информатизации и защите информации", Закон "О коммерческой тайне", Закон "О банках и банковской деятельности в РФ"и др.).
3. Цели защиты информации.
4. Экономические и моральные последствия атаки на информацию.
5. Пять уровней обеспечения информационной безопасности (системы защиты): Законодательный, Морально-этический, Административный, Физический, Аппаратно-программный.
6. Основные принципы выстраивания надежной системы защиты.
7. Понятие и виды защищаемой информации по законодательству Российской Федерации.
8. Понятие государственной, коммерческой, личной тайны. Основные нормативные документы в этой области.
9. Рассекречивание документов.
10. Международное законодательство в области защиты информации. Стандарты в области информационной безопасности.
11. Международные стандарты информационного обмена.

Тема 2.

1. Модели оценки ценности информации.
2. Классификация и общий анализ угроз безопасности информации.
3. Причины, виды, каналы утечки и искажения информации.
4. Основные методы реализации угроз информационной безопасности: методы нарушения конфиденциальности, целостности и доступности информации.
5. Модель нарушителя.

6. Угрозы секретности (конфиденциальности) информации: разглашение, утечка, несанкционированный доступ.
7. История появления компьютерных вирусов и факторы, влияющие на их распространение.
8. Вирусы как класс вредоносного программного обеспечения.
9. Классификация компьютерных вирусов.
10. Классификация компьютерных преступлений.
11. Понятие нарушителя информационной безопасности.
12. Виды хакеров.

Тема 3.

1. Схема построения информационной безопасности на уровне государства.
2. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации.
3. Национальные интересы Российской Федерации в информационной сфере и их обеспечение.
4. Интересы личности в информационной сфере.
5. Интересы общества в информационной сфере.
6. Интересы государства в информационной сфере.
7. Основные составляющие национальных интересов Российской Федерации в информационной сфере.
8. Виды угроз информационной безопасности Российской Федерации.
9. Источники угроз информационной безопасности Российской Федерации.
10. Направления обеспечения информационной безопасности государства.
11. Проблемы региональной информационной безопасности
12. Особенности обеспечения информационной безопасности в правоохранительных органах.

Тема4.

1. Сущность и перечень организационных мер по защите информации.
2. Субъекты деятельности по защите информации.
3. Структура и задачи подразделения по защите информации.
4. Сущность и перечень инженерно-технических мер по защите информации.
5. Методика и средства защиты информации.
6. Средства контроля эффективности защиты информации.
7. Средства физической защиты информации.
8. Классификация программных средств защиты информации.
9. Использование программ для обеспечения безопасности конфиденциальной информации.
10. Технологии защиты программного обеспечения.
11. Защита информации от утечки, несанкционированного доступа и несанкционированного воздействия.
12. Защита информации от непреднамеренного воздействия, разглашения и разведки.
13. Аудит информационной безопасности.

Тема 5.

1. Проблемы обеспечения безопасности обработки и хранения информации в вычислительных системах.
2. Базовые этапы построения системы комплексной защиты вычислительных систем.
3. Угрозы информационно-программному обеспечению вычислительных систем и их классификация.
4. Классификация методов защиты информации с использованием программно-аппаратных средств вычислительной системы.
5. Организационная структура системы комплексной защиты информационно-программного обеспечения.

6. Подходы к построению защищенной операционной системы.
7. Виды уязвимости и атак на операционные системы.
8. Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам.
9. Способы разграничения доступа к компьютерным ресурсам.
10. Защита программных средств от несанкционированного копирования, исследования и модификации.
11. Защита офисных документов.
12. Привязка программ к среде функционирования.
13. Защита программ от несанкционированного запуска.
14. Защита от деструктивных действий и размножения вирусов.
15. Использование средств аппаратного и программного контроля.
16. Технология гарантированного восстановление вычислительной системы после заражения компьютерными вирусами.

Тема 6.

1. Компьютерные сети, топология сетей, структура Интернет.
2. Принципы передачи информации в сети (протокол TCP/IP, доменная система имен, пакеты, порты, сетевые службы).
3. Защита Интернет-подключений.
4. Функции межсетевых экранов, понятие брандмауэра.
5. Технологии межсетевых экранов (фильтрация пакетов, применение шлюзов, прочие компоненты брандмауэров (файрволлов).
6. Брандмауэр Windows, настройка и определение правил.
7. Выявление следов несанкционированного доступа к файлам.
8. Сканеры и автоматизация поиска слабых мест в защите сети и в защите системы.
9. Анализаторы протоколов.
10. Возможности выявления и раскрытия преступлений в сфере компьютерной информации

Тема 7.

1. Основные понятия криптологии.
2. История шифрования.
3. Использование шифрования различными методами.
4. Симметричные и несимметричные системы шифрования информации.
5. Рассмотрение сокрытия информации таблицей Винжера.
6. Программы для криптографии.
7. Криптографические алгоритмы.
8. Электронная цифровая подпись (ЭЦП) и функция хэширования.
9. Создание и использование криптоключей.
10. Подтверждение подлинности объектов и субъектов информационной системы.
11. Понятие криптографической стойкости, вопросы практической стойкости.
12. Программно-аппаратные средства криптозащиты данных.

2.2. Перечень информационных источников по изучению разделов курса

Раздел 1. Учебники и учебные пособия, периодические и Интернет источники, рекомендованные автором курса в списке основной и дополнительной литературы.

Раздел 2. Учебники и учебные пособия, периодические и Интернет источники, рекомендованные автором курса в списке основной и дополнительной литературы.

Раздел 3. Учебники и учебные пособия, периодические и Интернет источники, рекомендованные автором курса в списке основной и дополнительной литературы.

Раздел 4. Учебники и учебные пособия, периодические и Интернет источники, рекомендованные автором курса в списке основной и дополнительной литературы.

Раздел 5. Учебники и учебные пособия, периодические и Интернет источники, рекомендованные автором курса в списке основной и дополнительной литературы.

Раздел 6. Учебники и учебные пособия, периодические и Интернет источники, рекомендованные автором курса в списке основной и дополнительной литературы.

Раздел 7. Учебники и учебные пособия, периодические и Интернет источники, рекомендованные автором курса в списке основной и дополнительной литературы.

2.3. Методические указания для обучающихся по освоению дисциплины

Цель методических рекомендаций - обеспечить студенту оптимальную организацию процесса изучения дисциплины, а также выполнения различных форм самостоятельной работы.

Основными видами учебной работы являются лекционные, практические занятия. Групповое обсуждение и индивидуальные консультации обучающихся в процессе решения учебных задач, в т.ч. посредством телекоммуникационных технологий. Обсуждение конкретных ситуаций. Просмотр и анализ учебных фильмов.

Успешное изучение дисциплины «Информационная безопасность» предполагает целенаправленную работу обучающихся над освоением ее теоретического содержания, предусмотренного учебной программой, активное участие в подготовке и проведении активных форм учебных занятий. В связи с этим обучающиеся должны руководствоваться рядом методических указаний.

Во-первых, при изучении дисциплины следует опираться и уметь конспектировать лекции, так как в учебниках, как правило, излагаются общепринятые, устоявшиеся научные взгляды.

Во-вторых, обучающийся обязан целенаправленно готовиться к практическим занятиям.

В-третьих, обучающемуся следует внимательно ознакомиться: с содержанием УМК, рабочей программы дисциплины, с целями и задачами дисциплины, ее связями с другими дисциплинами образовательной программы, методическими разработками по данной дисциплине, имеющимся на образовательном портале и сайте кафедры, с графиком консультаций преподавателей кафедры.

Это позволит четко представлять круг изучаемых дисциплиной проблем, ее место и роль в подготовке бакалавра.

В-четвертых, качественное и в полном объеме изучение дисциплины возможно при активной работе в часы самостоятельной подготовки. Обучающийся должен использовать нормативные документы, научную литературу и другие источники, раскрывающие в полном объеме содержание дисциплины. Список основной и дополнительной литературы, сайтов интернета предлагается в УМК. При этом следует иметь в виду, что для глубокого изучения дисциплины необходима литература различных видов:

а) учебники, учебные и учебно-методические пособия, в том числе и электронные;

б) справочная литература – энциклопедии, словари, тематические, терминологические справочники, раскрывающие категориально-понятийный аппарат дисциплины.

Изучая учебную литературу, следует уяснить основное содержание той или иной проблемы.

Рекомендации по подготовке к лекционным занятиям (теоретический курс)

Изучение дисциплины требует систематического и последовательного накопления знаний, следовательно, пропуски отдельных тем не позволяют глубоко освоить предмет. Именно поэтому контроль над систематической работой студентов всегда находится в центре внимания кафедры.

Студентам необходимо:

- перед каждой лекцией просматривать рабочую программу дисциплины, что позволит сэкономить время на записывание темы лекции, ее основных вопросов, рекомендуемой литературы;
- на отдельные лекции приносить соответствующий материал на бумажных носителях, представленный лектором на портале или присланный на «электронный почтовый ящик группы» (таблицы, графики, схемы). Данный материал будет охарактеризован, прокомментирован, дополнен непосредственно на лекции;
- перед очередной лекцией необходимо просмотреть по конспекту материал предыдущей лекции. При затруднениях в восприятии материала следует обратиться к основным литературным источникам. Если разобраться в материале опять не удалось, то обратитесь к лектору (по графику его консультаций) или к преподавателю на практических занятиях.

Методические рекомендации при работе над конспектом во время проведения лекции

В ходе лекционных занятий необходимо вести конспектирование учебного материала. Общие и утвердившиеся в практике правила и приемы конспектирования лекций:

- Конспектирование лекций ведется в специально отведенной для этого тетради, каждый лист которой должен иметь поля, на которых делаются пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.
- Необходимо записывать тему и план лекций, рекомендуемую литературу к теме. Записи разделов лекции должны иметь заголовки, подзаголовки, красные строки. Для выделения разделов, выводов, определений, основных идей можно использовать цветные карандаши и фломастеры.
- Названные в лекции ссылки на первоисточники надо пометить на полях, чтобы при самостоятельной работе найти и вписать их.
- В конспекте дословно записываются определения понятий, категорий и законов. Остальное должно быть записано своими словами.
- Каждому студенту необходимо выработать и использовать допустимые сокращения наиболее распространенных терминов и понятий.
- В конспект следует заносить всё, что преподаватель пишет на доске, а также рекомендуемые схемы, таблицы, диаграммы и т.д.

Методические рекомендации по подготовке к практическим занятиям

Целью практических занятий является углубление и закрепление теоретических знаний, полученных студентами на лекциях и в процессе самостоятельного изучения учебного материала, а, следовательно, формирование у них определенных умений и навыков.

В ходе подготовки к практическому занятию необходимо прочитать конспект лекции, изучить основную литературу, ознакомиться с дополнительной литературой, выполнить выданные преподавателем практические задания. При этом учесть рекомендации преподавателя и требования программы. Желательно при подготовке к практическим занятиям по дисциплине одновременно использовать несколько источников, раскрывающих заданные вопросы.

Методические рекомендации по выполнению различных форм промежуточного и итогового контроля

Для успешного усвоения курса необходимо не только посещать аудиторные занятия, но и вести активную самостоятельную работу. Самостоятельная работа студентов включает в себя выполнение различного рода заданий, которые ориентированы на более глубокое

усвоение материала изучаемой дисциплины. По каждой теме учебной дисциплины студентам предлагается перечень заданий для самостоятельной работы.

К выполнению заданий для самостоятельной работы предъявляются следующие требования: задания должны исполняться самостоятельно и представляться в установленный срок, а также соответствовать установленным требованиям по оформлению.

Студентам следует:

- руководствоваться графиком самостоятельной работы, определенным рабочей программы дисциплины;
- выполнять все плановые задания, выдаваемые преподавателем для самостоятельного выполнения, и разбирать на семинарах и консультациях неясные вопросы;
- использовать при подготовке методические разработки кафедры по написанию рефератов, эссе, контрольных работ;
- при подготовке к промежуточному и итоговому контролю параллельно прорабатывать соответствующие теоретические и практические разделы дисциплины, фиксируя неясные моменты для их обсуждения на плановой консультации, а также изучить определения всех понятий и теоретические подходы до состояния понимания материала по всем изученным темам.

Методические рекомендации по работе с литературой

Любая форма самостоятельной работы студента (подготовка к семинарскому занятию, написание эссе, контрольной работы, доклада и т.п.) начинается с изучения соответствующей литературы как в библиотеке, так и дома. К каждой теме учебной дисциплины подобрана основная и дополнительная литература. Основная литература - это учебники и учебные пособия. Дополнительная литература - это монографии, сборники научных трудов, журнальные и газетные статьи, различные справочники, энциклопедии, интернет-ресурсы.

Изучение дисциплины следует начинать с учебника, поскольку учебник – это книга, в которой изложены основы научных знаний по определенному предмету в соответствии с целями и задачами обучения, установленными программой.

Выбранную монографию или статью целесообразно внимательно просмотреть. В книгах следует ознакомиться с оглавлением и научно-справочным аппаратом, прочитать аннотацию и предисловие. Целесообразно ее пролистать, рассмотреть иллюстрации, таблицы, диаграммы, приложения. Такое поверхностное ознакомление позволит узнать, какие главы следует читать внимательно, а какие прочитать быстро.

При работе с литературой следует учитывать, что имеются различные виды чтения, и каждый из них используется на определенных этапах освоения материала.

Предварительное чтение направлено на выявление в тексте незнакомых терминов и поиск их значения в справочной литературе. В частности, при чтении указанной литературы необходимо подробнейшим образом анализировать понятия.

Сквозное чтение предполагает прочтение материала от начала до конца. Сквозное чтение литературы из приведенного списка дает возможность студенту сформировать свод основных понятий из изучаемой области и свободно владеть ими.

Выборочное – наоборот, имеет целью поиск и отбор материала. В рамках данного курса выборочное чтение, как способ освоения содержания курса, должно использоваться при подготовке к практическим занятиям по соответствующим разделам.

Аналитическое чтение – это критический разбор текста с последующим его конспектированием. Освоение указанных понятий будет наиболее эффективным в том случае, если при чтении текстов студент будет задавать к этим текстам вопросы. Часть из этих вопросов сформулирована в приведенном в ФОС перечне вопросов для собеседования.

Перечень этих вопросов ограничен, поэтому важно не только содержание вопросов, но сам принцип освоения литературы с помощью вопросов к текстам.

Целью изучающего чтения является глубокое и всестороннее понимание учебной информации.

Есть несколько приемов изучающего чтения:

1. Чтение по алгоритму предполагает разбиение информации на блоки: название; автор; источник; основная идея текста; фактический материал; анализ текста путем сопоставления имеющихся точек зрения по рассматриваемым вопросам; новизна.
2. Прием постановки вопросов к тексту имеет следующий алгоритм:
   - медленно прочитать текст, стараясь понять смысл изложенного;
   - выделить ключевые слова в тексте;
   - постараться понять основные идеи, подтекст и общий замысел автора.
3. Прием тезирования заключается в формулировании тезисов в виде положений, утверждений, выводов.

К этому можно добавить и иные приемы: прием реферирования, прием комментирования.

Для облегчения работы в книге или журнале, принадлежащим самому студенту, ключевые позиции можно выделять маркером или делать пометки на полях. При работе с Интернет-источником целесообразно также выделять важную информацию. Если же книга или журнал не являются собственностью студента, то целесообразно записывать номера страниц, которые привлекли внимание. Позже следует возвратиться к ним, перечитать или переписать нужную информацию. Физическое действие по записыванию помогает прочно заложить данную информацию в «банк памяти».

Выделяются следующие виды записей при работе с литературой:

Конспект - краткая схематическая запись основного содержания научной работы. Целью является не переписывание произведения, а выявление его логики, системы доказательств, основных выводов. Хороший конспект должен сочетать полноту изложения с краткостью.

Цитата - точное воспроизведение текста. Заключается в кавычки. Точно указывается страница источника.

Тезисы - концентрированное изложение основных положений прочитанного материала.

Аннотация - очень краткое изложение содержания прочитанной работы.

Резюме - наиболее общие выводы и положения работы, ее концептуальные итоги. Записи в той или иной форме не только способствуют пониманию и усвоению изучаемого материала, но и помогают вырабатывать навыки ясного изложения в письменной форме тех или иных теоретических вопросов.

Важной составляющей любого солидного научного издания является список литературы, на которую ссылается автор. При возникновении интереса к какой-то обсуждаемой в тексте проблеме всегда есть возможность обратиться к списку относящейся к ней литературы. При этом важно не терять из вида общий контекст и не погружаться чрезмерно в детали, потому что таким образом можно не увидеть главного.

2.4. Словарь (глоссарий) основных терминов и понятий

Информационная безопасность – это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации.

Защита информации – это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Доступность – это гарантия получения требуемой информации или информационной услуги пользователем за определенное время.
Целостность – гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений.
Конфиденциальность – гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена.
Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.
Система защиты государственной тайны – совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях.
Средства защиты информации – технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.
Политика безопасности – это комплекс предупредительных мер по обеспечению информационной безопасности организации. Политика безопасности включает правила, процедуры и руководящие принципы в области безопасности, которыми руководствуется организация в своей деятельности.
Угроза «информационной безопасности» – это потенциальная возможность нарушения режима информационной безопасности. Преднамеренная реализация угрозы называется ***атакой*** на информационную систему.
Программный вирус – это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах.
Удаленная угроза – потенциально возможное информационное разрушающее воздействие на распределенную вычислительную сеть, осуществляемая программно по каналам связи.
Идентификация – присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.
Аутентификация (установление подлинности) – проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности.
Электронная цифровая подпись – представляет собой относительно небольшое количество дополнительной аутентифи-цирующей информации, передаваемой вместе с подписываемым текстом.
Аудит – это анализ накопленной информации, проводимый оперативно, в реальном времени или периодически (например, раз в день).
Активный аудит – оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации.
Межсетевой экран (брандмауэр, firewall) – это программная или программно-аппаратная система, которая контролирует информационные потоки, поступающие в информационную систему и/или выходящие из нее, также обеспечивает защиту информационной системы посредством фильтрации информации. Фильтрация информации состоит в анализе информации по совокупности критериев и принятии решения о ее приеме и/или передаче.

2.5. Задания для самостоятельной работы по темам

Наименование темы или раздела дисциплины (модуля)	Задания для самостоятельной работы
Тема 1. Современное состояние и правовое регулирование сферы информационной безопасности.	Основные понятия и цели обеспечения информационной безопасности. Правовая основа обеспечения информационной безопасности. Основные положения Федерального закона «Об информации, информационных технологиях и о защите информации».
Тема 2. Место информационной безопасности экономических систем в национальной безопасности страны.	Основные положения Доктрины информационной безопасности Российской Федерации. Понятие защиты информации и виды защищаемой информации. Угрозы информационной безопасности в профессиональной сфере. Задача обеспечения информационной безопасности, как составная часть борьбы с преступностью.
Тема 3. Угрозы информационной безопасности и методы их реализации.	Виды каналов утечки информации. Доступность, целостность, конфиденциальность. Компьютерное преступление жизненный цикл информационных систем Понятие вируса и троянской программы, средства защиты от разрушающих воздействий вредоносных программ.
Тема 4. Способы и средства обеспечения защиты информации.	Сложные системы. Структурный подход. Угроза, атака, уязвимость, окно опасности, источник угрозы, злоумышленник. Основные угрозы доступности. Основные угрозы целостности. Основные угрозы конфиденциальности.
Тема 5. Информационная безопасность автоматизированных систем.	Угрозы безопасности информации, обрабатываемой в автоматизированных системах. Основные принципы и направления защиты автоматизированных систем от несанкционированного доступа. Методы ограничения доступа к информации, обрабатываемой в автоматизированных системах.
Тема 6. Безопасность компьютерных сетей.	Компьютерные сети, структура сети Интернет. Протокол передачи данных TCP/IP (IP-адрес, доменное имя). Сетевые службы (WWW, почта, FTP), пакеты, порты. Ресурсы общего доступа в сети, разграничение прав доступа. Механизмы защиты от сетевых атак. Понятие брандмауэр, правила файрвола. Источники информации о сетевых атаках (журналы регистрации событий, сетевой трафик и т.п.). Экранирование. Фильтрация. Межсетевые экраны. Механизмы сокрытия пребывания абонента в сети Интернет.

Тема 7. Криптографическая защита информации.	Криптография как наука, симметричные и несимметричные алгоритмы шифрования. Криптография и стеганография. Особенности и отличия. Идентификация/аутентификация с помощью биометрических данных. Идентификация пользователя и аутентификация электронного сообщения. Понятие вируса и троянской программы, средства защиты от разрушающих воздействий вредоносных программ. Утилиты обслуживания компьютеров.

Раздел III. Контроль знаний и компетенций студента

3.1.Описание балльно-рейтинговой системы

Для успешного освоения дисциплины «Информационная безопасность» необходимо лекционные материалы дополнять самостоятельным изучением специальной литературы. Решение задач и кейсов по курсу является неотъемлемым условием овладения навыками анализа и принятия управленческих решений в страховой практике.

Текущий контроль успеваемости осуществляется путем оценки выполнения заданий по курсу. Промежуточные аттестации проводятся в форме контрольного тестирования и выполнения домашнего задания по каждой их тем курса. Итоговый контроль (экзамен) проводится в устной форме - оценивается ответ слушателя на 2 вопроса по теме курса.

Для контроля успеваемости используется балльно-рейтинговая система, в основе которой следующих результаты работы студентов:

- 10% финальной оценки зависит от работы на практической части занятий (на протяжении всей дисциплины) – 10 баллов, соответственно;
- 35% - от результатов контрольного тестирования по темам 1-7 - 35 баллов;
- 35% - от результатов выполнения домашнего задания по темам 1-7 -35 баллов;
- 20% - от результатов итогового контроля (экзамен) - 10 баллов.

Всего за семестр можно набрать 100 баллов.

Шкала оценок

Количество кредитов	Оценка	Неудовлетворительно		Удовлетворительно		Хорошо	Отлично	
4	Оценка ECTS	F(2)	FX(2+)	E(3)	D(3+)	C(4)	B(5)	A(5+)
	Максимум 100 баллов	Менее 31	31-50	51-60	61-68	69-85	86-94	95-100

3.2.Перечень рефератов и/или эссе работ по темам.

Домашнее задание выполняется слушателем самостоятельно. Список вопросов для подготовки домашнего задания, выдается для ознакомления на первом занятии по теме, тогда же преподавателем проводится предварительное распределение вопросов по слушателям (по-алфавиту, в соответствие со списком слушателей). На втором занятии проводится окончательное распределение вопросов по слушателям (в соответствие с пожеланиями слушателей) а также предоставляется методика оценки за домашнее задание. Домашнее задание подготавливается слушателем в письменном виде, форме эссе и сдается на последнем занятии по теме.

Критерии оценки домашнего задания:

- очевидна логика решения, ее соответствие изученным теоретическим основам, методам и инструментам анализа – 2 балла,
- правильно прописаны все этапы и использована соответствующая методология – 1 балл,
- продемонстрировано знание нормативной базы – 1 балл,
- выводы соответствуют полученным результатам, обоснованы и аргументированы – 1 балл.

Максимальная оценка за домашнее задание - 5 баллов.

Накопленная оценка за домашнее задание доводится преподавателем до слушателей (например, на электронную почту) перед экзаменом.

Перечень домашних заданий (эссе) по темам

Тема 1.

1. Основные задачи, решаемые при обеспечении информационной безопасности.
2. Законодательные основы по защите информации (Федеральный закон "Об информации, информатизации и защите информации", Закон "О коммерческой тайне", Закон "О банках и банковской деятельности в РФ"и др.).
3. Цели защиты информации.
4. Экономические и моральные последствия атаки на информацию.
5. Пять уровней обеспечения информационной безопасности (системы защиты): Законодательный, Морально-этический, Административный, Физический, Аппаратно-программный.
6. Основные принципы выстраивания надежной системы защиты.
7. Понятие и виды защищаемой информации по законодательству Российской Федерации.
8. Понятие государственной, коммерческой, личной тайны. Основные нормативные документы в этой области.
9. Рассекречивание документов.
10. Международное законодательство в области защиты информации. Стандарты в области информационной безопасности.
11. Международные стандарты информационного обмена.

Тема 2.

1. Модели оценки ценности информации.
2. Классификация и общий анализ угроз безопасности информации.
3. Причины, виды, каналы утечки и искажения информации.
4. Основные методы реализации угроз информационной безопасности: методы нарушения конфиденциальности, целостности и доступности информации.
5. Модель нарушителя.
6. Угрозы секретности (конфиденциальности) информации: разглашение, утечка, несанкционированный доступ.
7. История появления компьютерных вирусов и факторы, влияющие на их распространение.
8. Вирусы как класс вредоносного программного обеспечения.
9. Классификация компьютерных вирусов.
10. Классификация компьютерных преступлений.
11. Понятие нарушителя информационной безопасности.
12. Виды хакеров.

Тема 3.

1. Схема построения информационной безопасности на уровне государства.
2. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации.

3. Национальные интересы Российской Федерации в информационной сфере и их обеспечение.
4. Интересы личности в информационной сфере.
5. Интересы общества в информационной сфере.
6. Интересы государства в информационной сфере.
7. Основные составляющие национальных интересов Российской Федерации в информационной сфере.
8. Виды угроз информационной безопасности Российской Федерации.
9. Источники угроз информационной безопасности Российской Федерации.
10. Направления обеспечения информационной безопасности государства.
11. Проблемы региональной информационной безопасности
12. Особенности обеспечения информационной безопасности в правоохранительных органах.

Тема4.

1. Сущность и перечень организационных мер по защите информации.
2. Субъекты деятельности по защите информации.
3. Структура и задачи подразделения по защите информации.
4. Сущность и перечень инженерно-технических мер по защите информации.
5. Методика и средства защиты информации.
6. Средства контроля эффективности защиты информации.
7. Средства физической защиты информации.
8. Классификация программных средств защиты информации.
9. Использование программ для обеспечения безопасности конфиденциальной информации.
10. Технологии защиты программного обеспечения.
11. Защита информации от утечки, несанкционированного доступа и несанкционированного воздействия.
12. Защита информации от непреднамеренного воздействия, разглашения и разведки.
13. Аудит информационной безопасности.

Тема 5.

1. Проблемы обеспечения безопасности обработки и хранения информации в вычислительных системах.
2. Базовые этапы построения системы комплексной защиты вычислительных систем.
3. Угрозы информационно-программному обеспечению вычислительных систем и их классификация.
4. Классификация методов защиты информации с использованием программно-аппаратных средств вычислительной системы.
5. Организационная структура системы комплексной защиты информационно-программного обеспечения.
6. Подходы к построению защищенной операционной системы.
7. Виды уязвимости и атак на операционные системы.
8. Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам.
9. Способы разграничения доступа к компьютерным ресурсам.
10. Защита программных средств от несанкционированного копирования, исследования и модификации.
11. Защита офисных документов.
12. Привязка программ к среде функционирования.
13. Защита программ от несанкционированного запуска.
14. Защита от деструктивных действий и размножения вирусов.
15. Использование средств аппаратного и программного контроля.

16. Технология гарантированного восстановление вычислительной системы после заражения компьютерными вирусами.

Тема 6.

1. Компьютерные сети, топология сетей, структура Интернет.
2. Принципы передачи информации в сети (протокол TCP/IP, доменная система имен, пакеты, порты, сетевые службы).
3. Защита Интернет-подключений.
4. Функции межсетевых экранов, понятие брандмауэра.
5. Технологии межсетевых экранов (фильтрация пакетов, применение шлюзов, прочие компоненты брандмауэров (файрволлов).
6. Брандмауэр Windows, настройка и определение правил.
7. Выявление следов несанкционированного доступа к файлам.
8. Сканеры и автоматизация поиска слабых мест в защите сети и в защите системы.
9. Анализаторы протоколов.
10. Возможности выявления и раскрытия преступлений в сфере компьютерной информации

Тема 7.

1. Основные понятия криптологии.
2. История шифрования.
3. Использование шифрования различными методами.
4. Симметричные и несимметричные системы шифрования информации.
5. Рассмотрение сокрытия информации таблицей Винжера.
6. Программы для криптографии.
7. Криптографические алгоритмы.
8. Электронная цифровая подпись (ЭЦП) и функция хэширования.
9. Создание и использование криптоключей.
10. Подтверждение подлинности объектов и субъектов информационной системы.
11. Понятие криптографической стойкости, вопросы практической стойкости.
12. Программно-аппаратные средства криптозащиты данных.

3.5. Описание показателей, критериев и шкалы оценивания компетенций и методические материалы, определяющие процедуры оценивания результатов освоения дисциплины

Работа на занятиях (активность слушателей) – оценивается участие слушателей в дискуссиях, правильность решения кейсов, ответы на вопросы преподавателя и т.д. по каждой из семи изучаемых тем. По первым четырем темам активность за каждое занятие оценивается в диапазоне от 0 до 1 балла, по пятому, шестому и седьмому - от 0 до 2 балов. Оценки за работу на аудиторных занятиях преподаватель выставляет в рабочую ведомость. Накопленная оценка (максимальная оценка за работу на занятиях - 10 баллов) определяется перед экзаменом и доводится преподавателем до слушателей (например, на электронную почту).

Контрольное тестирование – проводится в конце последнего занятия по теме занятии в течение 20 мин., и требует от слушателя ответа на вопрос в форме эссе, выбираемого преподавателем индивидуально для каждого слушателя по теме курса.

На первом занятии предоставляется методика проведения тестирования и проводится обзор примерных вопросов.

Критерии оценки эссе:

- очевидна логика решения, ее соответствие изученным теоретическим основам, методам и инструментам анализа – 2 балла,
- правильно прописаны все этапы и использована соответствующая методология – 1 балл,

- продемонстрировано знание нормативной базы – 1 балл,
- выводы соответствуют полученным результатам, обоснованы и аргументированы – 1 балл.

Максимальная оценка за контрольное тестирование - 5 баллов.

Накопленная оценка и за контрольное тестирование доводится преподавателем до слушателей (например, на электронную почту) перед экзаменом.

Для контроля успеваемости используется балльно-рейтинговая система, в основе которой следующих результаты работы студентов:

- 10% финальной оценки зависит от работы на практической части занятий (на протяжении всей дисциплины) – 10 баллов, соответственно;
- 35% - от результатов контрольного тестирования по темам 1-7 - 35 баллов;
- 35% - от результатов выполнения домашнего задания по темам 1-7 -35 баллов;
- 20% - от результатов итогового контроля (экзамен) - 10 баллов.

Всего за семестр можно набрать 100 баллов.

Итоговая оценка включает в себя накопленную оценку слушателя по всем формам контроля (максимальная накопленная оценка– 100 баллов).

Шкала оценок

Количество кредитов	Оценка	Неудовлетворительно		Удовлетворительно		Хорошо	Отлично	
4	Оценка ECTS	F(2)	FX(2+)	E(3)	D(3+)	C(4)	B(5)	A(5+)
	Максимум 100 баллов	Менее 31	31-50	51-60	61-68	69-85	86-94	95-100

Критерии оценки:

A – («Отлично»)– теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному.

B – («Очень хорошо») - теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом в основном формированы, все предусмотренные программой обучения учебные задания выполнены, качество выполнения большинства из них оценено числом баллов, близким к максимальному.

C – («Хорошо») - теоретическое содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения не одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками.

D – («Удовлетворительно») - теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий, возможно, содержат ошибки.

E – («Посредственно») - теоретическое содержание курса освоено частично, некоторые практические навыки работы не сформированы, многие предусмотренные программой обучения учебные задания не выполнены, либо качество выполнения некоторых из них оценено числом баллов, близким к минимальному.

FX – («Условно неудовлетворительно») - теоретическое содержание курса освоено частично, необходимые практические навыки работы не сформированы, большинство предусмотренных программой обучения учебных заданий не выполнены, либо качество их выполнения оценено числом баллов, близким к минимальному; при дополнительной самостоятельной работе над материалом курса возможно повышение качества выполнения учебных заданий.
F – («Безусловно неудовлетворительно») - теоретическое содержание курса не освоено, необходимые практические навыки работы не сформированы, все выполненные учебные задания содержат грубые ошибки, дополнительная самостоятельная работа над материалом курса не приведет какому-либо значимому повышению качества выполнения учебных заданий.

Программа составлена в соответствии с требованиями ОС ВО РУДН/ФГОС.

Разработчик:

. _____ Гусев А.И.
должность, название кафедры подпись инициалы, фамилия

Руководитель программы
Международная экономическая безопасность
Доц, к.э.н. _____ Глинская М.В.
подпись инициалы, фамилия