

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ
федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский Нижегородский государственный университет им.
Н.И. Лобачевского»

Институт экономики и предпринимательства

УТВЕРЖДЕНО
решением ученого совета ННГУ
протокол от
«14» декабря 2021 г. № 4

Рабочая программа дисциплины

Информационная безопасность

Уровень высшего образования
специалитет

Специальность
38.05.02 «Таможенное дело»

Специализация
Таможенные операции и таможенный контроль

Квалификация (степень) выпускника
Специалист таможенного дела

Форма обучения
Очная, заочная

2021 год

1. Место дисциплины (модуля) в структуре ОПОП.

Дисциплина относится к вариативной части ОПОП по специальности 38.05.02 «Таможенное дело» и является дисциплиной по выбору. Основное назначение данной дисциплины состоит в эффективном освоении теоретических основ обеспечения информационной безопасности организаций, формирование умения и практических навыков применения методов и средств защиты информации.

В связи с этим, основной задачей преподавания дисциплины «Информационная безопасность» является подготовка специалистов, обладающих знаниями, навыками, умениями в сфере обеспечения информационной безопасности организаций различных форм собственности.

Минимальный уровень освоения содержания дисциплины предполагает:

- Знакомство с основными понятиями информационной безопасности, информационными угрозами, их классификацией, и возможными последствиями для организаций различных форм собственности;
- Уяснение вопросов обеспечения информационной безопасности организации и проблем создания (концептуального проектирования) систем информационной безопасности;
- Принятие обоснованных решений по выбору политики информационной безопасности (ИБ) и оценки эффективности инвестиций в ИБ.

Тематическим планом преподавания дисциплины предусматриваются следующие виды занятий: лекции, практические занятия, самостоятельная работа. Контроль знаний обучающихся осуществляется в ходе тестирования и сдачи зачета.

Знания, навыки и умения, приобретенные в процессе изучения дисциплины в ходе лекций, практических занятий и самостоятельной работы, должны всесторонне использоваться студентами на завершающем этапе обучения в специалитете, при обучении в магистратуре, а также в процессе дальнейшей профессиональной деятельности при решении широкого класса аналитических задач финансово-экономического характера.

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников).

Формируемые компетенции (код компетенции, уровень освоения – при наличии в карте компетенции)	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций
ОПК-1 способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (этап формирования компетенции - базовый)	<i>З1 (ОПК-1) Знать:</i> основные методы, способы и средства преобразования информации <i>У1 (ОПК-1) Уметь:</i> работать с компьютером как средством управления информацией <i>В1 (ОПК-1) Владеть:</i> основными способами обнаружения информационных угроз и использования современных анти-вирусных программ
ПК-3 способность владением навыками применения технических средств таможенного контроля и эксплуатации оборудования и приборов (этап формирования компетенции – начальный)	<i>З1 (ПК-3) Знать</i> общие основы использования компьютерных систем; <i>У1 (ПК-3) Уметь</i> применять компьютерные системы для решения задач профессиональной деятельности; <i>В1 (ПК-3) Владеть</i> навыками применять компьютерные системы для решения, связанных с эксплуатацией технических средств

ПК-25: способность организовывать сбор информации для управленческой деятельности, оценивать эффективность деятельности таможен (таможенного поста) и их структурных подразделений, анализировать качество предоставляемых услуг (<i>этап формирования компетенции – начальный</i>)	<p><i>З1 (ПК-25) Знать</i> структуру, содержание и основные понятия информационной среды и требования информационной безопасности;</p> <p><i>У1 (ПК-25) Уметь</i> применять информационно-коммуникационные технологии к решению задач профессиональной деятельности с учетом требований информационной безопасности;</p> <p><i>В1 (ПК-25) Владеть</i> навыками сбора информации с учетом требований информационной безопасности</p>
ПК-32 владение навыками применения в таможенном деле информационных технологий и средств обеспечения их функционирования в целях информационного сопровождения профессиональной деятельности (<i>этап формирования компетенции - начальный, базовый</i>)	<p>Знать: теоретические аспекты информационной безопасности (ИБ) экономических систем</p> <p>типы информационных угроз и их характеристики</p> <p>организацию системы защиты информации экономических систем</p> <p>Уметь: формулировать цели и задачи защиты информации экономических объектов</p> <p>принимать обоснованные решения по выбору политики безопасности и оценке эффективности инвестиций в ИБ</p> <p>работать в среде специализированных программных комплексов и систем, применяемых в ИБ</p> <p>Владеть: методами развития комплексов и технологий ИБ подходами к организации ИБ экономических систем.</p>
ПК-34: способностью обеспечивать информацией в сфере таможенного дела государственные органы, организации и отдельных граждан (<i>этап формирования компетенции – начальный, базовый</i>)	<p><i>З1 (ПК-34) Знать</i> виды современных информационных технологий, используемых таможенными органами с целью обеспечения информацией в сфере таможенного дела государственные органы, организации и отдельных граждан, и требования безопасности к ним</p> <p><i>У1 (ПК-34) Уметь</i> работать в среде специализированных программных комплексов и систем, применяемых таможенными органами в сфере их профессиональной деятельности с учетом требований информационной безопасности;</p> <p><i>В1 (ПК-34) Владеть</i> современными ИТ – технологиями, используемыми таможенными органами с целью обеспечения информацией в сфере таможенного дела государственные органы, организации и отдельных граждан с учетом требований информационной безопасности</p>
ПК-35: владением навыками использования электронных способов обмена информацией и средств их обеспечения, применяемых таможенными органами (<i>этап формирования компетенции – начальный, базовый</i>)	<p><i>З1 (ПК-35) Знать</i> виды современных информационных технологий, используемых таможенными органами с целью обмена необходимой информацией, и требования безопасности к ним</p> <p><i>У1 (ПК-35) Уметь</i> работать в среде специализированных программных комплексов и систем, применяемых таможенными органами в сфере их профессиональной деятельности с учетом требований информационной безопасности;</p> <p><i>В1 (ПК-35) Владеть</i> современными ИТ – технологиями, используемыми таможенными органами для обмена информацией в рамках профессиональной деятельности с учетом требований информационной безопасности</p>

Формы промежуточной аттестации: зачет.

3. Структура и содержание дисциплины (модуля).

Объем дисциплины составляет 3 зачетные единицы, всего 108 часов, из которых по очной форме обучения: 49 часов составляет контактная работа обучающегося с преподавателем (16 часов занятия лекционного типа, 32 часа занятия лабораторного типа (научно-практические занятия, лабораторные работы и т.п.), 59 часов составляет самостоятельная работа обучающегося в виде рефератов, ознакомления с нормативно-правовой документацией по информационной безопасности.

По заочной форме обучения 13 часов составляет контактная работа обучающегося с преподавателем (4 часа занятия лекционного типа, 8 часов занятия лабораторного типа (науч-

но-практические занятия, лабораторные работы и т.п.), 91 час составляет самостоятельная работа обучающегося в виде рефератов, ознакомления с нормативно-правовой документацией по информационной безопасности.

Структура и содержание дисциплины (модуля)

Наименование и краткое содержание разделов и тем дисциплины (модуля), форма промежуточной аттестации по дисциплине (модулю)	Всего (часы)			В том числе																	
				Контактная работа (работа во взаимодействии с преподавателем), часы из них											Самостоятельная работа обучающегося, часы			КСР			
				Занятия лекционного типа			Занятия семинарского типа			Занятия лабораторного типа			Консультации						Всего		
	Очная	Очно-заочная	Заочная	Очная	Очно-заочная	Заочная	Очная	Очно-заочная	Заочная	Очная	Очно-заочная	Заочная	Очная	Очно-заочная	Заочная	Очная	Очно-заочная	Заочная	Очная	Очно-заочная	Заочная
Тема 1. Теоретические аспекты ИБ экономических систем	16		17	2		1	4		1						6		2	10		15	
Тема 2. Понятие информационных угроз и их виды	16		17	2		1	4		1						6		2	10		15	
Тема 3. Государственное регулирование ИБ	16		18	2		1	4		2						6		3	10		15	
Тема 4. Подходы, принципы, методы и средства обеспечения безопасности	16		18	2		1	4		2						6		3	10		15	
Тема 5. Организация системы защиты информации	22		16	4			8		1			2			12		1	10		15	
Тема 6. Менеджмент и аудит систем ИБ	21		15	4			8		1			2			12		1	9		14	1
Текущий контроль	2						2														1
Промежуточная аттестация: зачет																					
Итого	108		108	16		4	32		8						48		12	59		91	1

В случае, когда дисциплина (модуль) полностью формирует какую-то компетенцию и (или) завершает формирование компетенции, одним из разделов дисциплины (модуля) может быть выполнение проекта, формирование портфолио или другой вид комплексной проверки сформированности компетенции в целом

Тема 1. Теоретические аспекты информационной безопасности экономических систем

Информационное общество. Информационное пространство. Информационная война и информационное противоборство. Информационная преступность. Угрозы безопасности информации. Информационная безопасность (ИБ). Политика безопасности. Объекты и субъекты обеспечения ИБ. Методы и средства обеспечения ИБ. Объекты ИБ на предприятии. Системный подход к защите информации. Структура (подсистемы) системы ИБ. Экономическая информация как товар и объект безопасности.

Информационные ресурсы и информационная безопасность. Правовой режим информационных ресурсов. Информационно-правовые отношения. Документирование информации как обязательное условие включения информации в информационные ресурсы. Понятие ценной (собственной) предпринимательской информации. Ценность и полезность информации. Критерии ценности информационных ресурсов. Правовые и экономические предпосылки выделения ценной информации. Взаимосвязь критериев ценности и необходимости обеспечения безопасности информации. Понятие уязвимости информации. Типовые классификационные группы ценной предпринимательской информации. Информационные ресурсы государственные и негосударственные. Классификация информационных продуктов и услуг. Информационные ресурсы открытые и ресурсы ограниченного доступа и использования.

Тема 2. Понятие информационных угроз и их виды

Информационные угрозы. Угрозы нарушения конфиденциальности информации. Информационная атака. Потенциальные злоумышленники (хакеры, крэкеры). Информационные угрозы для государства, для компании (юридического лица), для личности (физического лица). Естественные и человеческие факторы информационных угроз (ИУ). Классификация угроз безопасности информации. Несанкционированный доступ к защищаемой информации. Типовые пути несанкционированного доступа к информации. Вредоносные программы. Разглашение и утечка конфиденциальной информации (КИ). Каналы утечки КИ. Исторические аспекты реализации информационных угроз. Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации угроз ИБ. Способы воздействия угроз на информационные объекты. Проявления возможного ущерба. Идентификация угроз. Компьютерные преступления и наказания. Исторические примеры и современность. Риски угроз информационным ресурсам. **Тема 3. Государственное регулирование информационной безопасности**

Ущерб от компьютерных злоупотреблений. Исторические аспекты борьбы органов уголовной юстиции с компьютерной преступностью (опыт США, стран Западной Европы, России). Меры, направленные на создание и поддержание в обществе негативного (в том числе карательного) отношения к нарушениям и нарушителям информационной безопасности. Международные договоры, доктрины в области ИБ. Информационные права граждан. Основные законодательные по ИБ физических и юридических лиц в России (Конституция РФ, федеральные законы, Уголовный кодекс, Налоговый кодекс, Гражданский кодекс и др.). Специальное законодательство в области информатизации информационных технологий и информационной безопасности – федеральные законы, их структура и содержание. Доктрина информационной безопасности России, принятая в 2016 году. Стандарты информационной безопасности. Правовые нормы ИБ в организациях. Законодательство в области интеллектуальной собственности, информационных ресурсов, информационных продуктов.

Повышение образовательной и правовой культуры населения в сфере ИБ.

Тема 4. Подходы, принципы, методы и средства обеспечения безопасности

Управление защитой информации. Фрагментарный и комплексный подходы к защите информации. Характеристики методов средств ИБ экономического объекта. Криптография, механизмы цифровой подписи и особенности ее применения. Идентификация и аутентификация. Разграничения доступа. Протоколирование и аудит. Организационно-техническое обеспечение компьютерной безопасности. Организация конфиденциального делопроизводства. Программно-технические методы защиты информации. Виды служб безопасности, их место в аппарате управления предпринимательских структур различных типов. Менеджер по безопасности. Задачи службы безопасности, основные функции. Руководство и подчиненность. Типовая структура службы безопасности. Место, задачи, функции и структура подразделения (или службы) конфиденциальной документации. Задачи и функции аналитического подразделения. Задачи и функции подразделения охраны и пропускного режима. Задачи и функции подразделения инженерно-технической защиты информации. Задачи и функции других подразделений. Взаимодействие службы безопасности и службы персонала. Организационные формы обеспечения безопасности в некрупных фирмах и малом бизнесе. Профессиональные и психологические требования к сотрудникам службы безопасности. Плановая и контрольная работа в службе безопасности. Назначение и взаимосвязь плановой и контрольной работы службы безопасности. Их место в построении и функционировании комплексной системы защиты информации фирмы. Анализ и оценка надежности и эффективности применяемой системы защиты. Регламентированный и нерегламентированный контроль системы защиты. Цели и задачи планирования работы по формированию и совершенствованию системы защиты информации. Планирование работы службы. Стадии контроля; учет контрольных операций. Методы и средства защиты от вредоносных программ. Профилактика вирусного заражения программ. Защита информации в Интернете.

Тема 5. Организация системы защиты информации

Политика информационной безопасности. Принципы реализации политики безопасности. Этапы построения системы ИБ. Способы устранения (смягчения) воздействия непредвиденных ситуаций. Обеспечение ИБ автоматизированных банковских систем, электронной коммерции и др.

Тема 6. Менеджмент и аудит систем информационной безопасности

Оценка эффективности инвестиций в информационную безопасность.

Основные принципы управления рисками информационной безопасности:

Шестнадцать методов, используемые для реализации пяти принципов управления рисками. Оценка риска и определение потребности. Признание информационных ресурсов в качестве существенных (неотъемлемых) активов организации. Разработка практических процедур оценки рисков, связывающих безопасность и требования бизнеса. Ответственность менеджеров бизнес-подразделений и менеджеров, участвующих в программе обеспечения безопасности. Непрерывное управление рисками. Централизованное управление. Определение бюджета и персонала. Профессионализм и технические знания сотрудников. Средства контроля. Контроль факторов, влияющих на риски и указывающих на эффективность информационной безопасности. Новые методы и средства контроля.

4. Образовательные технологии

Реализация компетентностного подхода при изучении дисциплины «Информационная безопасность» предполагает широкое использование в учебном процессе активных и интерактивных форм проведения занятий (компьютерных программ, деловых игр по актуальным проблемам, разбор конкретных ситуаций) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков студентов. В рамках данного курса возможны встречи с представителями компаний различных форм собственности, государственных и муниципальных органов.

Все занятия, проводимые по дисциплине, в том числе и самостоятельная работа студентов, предусматривают сочетание передовых методических приемов с новыми образовательными информационными технологиями.

На занятиях используются современные формы и методы обучения (тренинги, исследовательские методы, проблемное и проектное обучение), направленные на развитие творческих способностей и самостоятельности студентов, привитие им интереса к исследовательской работе, формирование убеждения о необходимости при решении любых прикладных задач использования инновационных информационных технологий.

Лекционные занятия проводятся в специализированных аудиториях с применением мультимедийных технологий и предусматривают развитие полученных теоретических знаний с использованием рекомендованной учебной литературы и других источников информации, в том числе информационных ресурсов сети Интернет.

Практические занятия проводятся в компьютерных классах с применением специализированных информационных систем, комплексов и технологий бизнес-индустрии.

Тематика практических заданий ориентирована на рассмотрение аналитических типовых и исследовательских задач финансово-экономического характера.

В ходе самостоятельной работы, при подготовке к плановым занятиям, экзамену студенты анализируют поставленные преподавателем задачи и проблемы и с использованием учебно-методической литературы, информационных систем, комплексов и технологий, материалов, найденных в глобальной сети Интернет, находят пути их разрешения.

Профессорско-педагогический состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ограниченными возможностями здоровья, индивидуальными программами реабилитации инвалидов (при наличии). При необходимости осуществляется дополнительная поддержка преподавания тьюторами, психологами, социальными работниками, прошедшими подготовку ассистентами.

В соответствии с методическими рекомендациями Минобрнауки РФ (утв. 8 апреля 2014 г. N АК-44/05вн) в курсе предполагается использовать социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Подбор и разработка учебных материалов производятся с учетом предоставления материала в различных формах: аудиальной, визуальной, с использованием специальных технических средств и информационных систем.

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения

общего и специального назначения (персонального и коллективного использования). Материально-техническое обеспечение предусматривает приспособление аудиторий к нуждам лиц с ОВЗ.

Форма проведения аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей. Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной или электронной форме (для лиц с нарушениями опорно-двигательного аппарата);
- в печатной форме или электронной форме с увеличенным шрифтом и контрастностью (для лиц с нарушениями слуха, речи, зрения);
- методом чтения ассистентом задания вслух (для лиц с нарушениями зрения).

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге или набором ответов на компьютере (для лиц с нарушениями слуха, речи);
- выбором ответа из возможных вариантов с использованием услуг ассистента (для лиц с нарушениями опорно-двигательного аппарата);
- устно (для лиц с нарушениями зрения, опорно-двигательного аппарата).

5. Учебно-методическое обеспечение самостоятельной работы обучающихся

5.1. Рекомендации преподавателю

В ходе изучения дисциплины уделяется внимание как теоретическому усвоению понятий информационной безопасности, так и приобретению, развитию и закреплению практических навыков и умений по использованию специализированных информационных средств и технологий при организации ИБ экономических систем.

На лекциях раскрываются основные вопросы рассматриваемой темы, делаются акценты на наиболее важные, сложные и проблемные положения изучаемого материала, которые должны быть приняты студентами во внимание.

На практических занятиях, ориентированных на предметную область будущей профессиональной деятельности студентов, выборочно контролируется степень усвоения студентами основных теоретических положений. Рассматривается технология применения аппаратно-программных средств для организации ИБ. При решении практических заданий используются не только инструментальные средства информационных технологий бизнес-индустрии, но и методы и понятия дисциплин финансово-экономического блока.

После изучения каждой темы предусматривается выполнение студентами самостоятельной работы с проверкой как степени усвоения ими теоретических знаний, так и объема и качества приобретенных практических навыков и умений.

5.2. Рекомендации студентам

Для лучшего усвоения положений дисциплины студенты должны:

- постоянно и систематически, с использованием рекомендованной литературы и электронных источников информации, закреплять знания, полученные на лекциях;
- находить решения проблемных вопросов, поставленных преподавателем в ходе лекций и практических заданий;
- регулярно и своевременно изучать материал, выданный преподавателем на самостоятельную проработку;
- с использованием средств информационных систем, комплексов и технологий, электронных учебников и практикумов, справочных правовых и тренинго-тестирующих си-

стем, информационных ресурсов сети Интернет выполнить на компьютере тематические практические задания, предназначенные для самостоятельной работы;

- находить, используя разные источники информации, ответы на теоретические и практические контрольные вопросы по темам дисциплины;
- использовать информацию, найденную на сайтах фирм–разработчиков информационных систем и технологий, применяемых в экономике;
- при подготовке к экзамену учитывать общие требования и рекомендации.

При освоении данного курса специалистам может быть предложено выполнение инициативной научно-исследовательской работы.

Методические указания по выполнению научно-исследовательской работы

Целью выполнения работы является:

- закрепление знаний, полученных студентами в процессе теоретического обучения;
- проведение исследования проблемы;
- активное использование пакетов прикладных программ; анализ библиографических материалов.
- отработка приемов и способов аналитических расчетов на практическом материале.

Выбор темы производится студентом и утверждается преподавателем. Рекомендуемый объем работы 10-15 страниц машинописного текста.

В каждой работе, кроме основных разделов, независимо от темы, предусматривается «Введение», «Заключение», «Список используемой литературы», «Приложения».

Список литературы должен быть составлен в соответствии с библиографическими требованиями.

Выполнять научно-исследовательскую работу необходимо с использованием текстового редактора MS Word, электронных таблиц Excel, а также можно использовать пакеты прикладных программ (ППП).

К оформлению научно-исследовательской работы предъявляются общие типовые требования.

Рекомендуемые направления научно-исследовательских работ

- 1 Информационное право и информационная безопасность.
- 2 Концепция информационной безопасности.
- 3 Анализ законодательных актов об охране информационных ресурсов открытого доступа.
- 4 Анализ законодательных актов о защите информационных ресурсов ограниченного доступа.
- 5 Соотношение понятий: информационные ресурсы, информационные системы и информационная безопасность.
- 6 Информационная безопасность (по материалам зарубежных источников и литературы).
- 7 Правовые основы защиты конфиденциальной информации.
- 8 Экономические основы защиты конфиденциальной информации.
- 9 Организационные основы защиты конфиденциальной информации.
- 10 Структура, содержание и методика составления перечня сведений, относящихся к предпринимательской тайне.
- 11 Составление инструкции по обработке и хранению конфиденциальных документов.
- 12 Направления и методы защиты документов на бумажных носителях.
- 13 Направления и методы защиты машиночитаемых документов.
- 14 Архивное хранение конфиденциальных документов.
- 15 Направления и методы защиты аудио- и визуальных документов.

- 16 Порядок подбора персонала для работы с конфиденциальной информацией.
- 17 Методика тестирования и проведения собеседования с претендентами на должность, связанную с секретами фирмы.
- 18 Назначение, структура и методика построения разрешительной системы доступа персонала к секретам фирмы.
- 19 Порядок проведения переговоров и совещаний по конфиденциальным вопросам.
- 20 Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний.
- 21 Порядок работы с посетителями фирмы, организационные и технические методы защиты секретов фирмы.
- 22 Порядок защиты информации в рекламной и выставочной деятельности.
- 23 Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.
- 24 Анализ источников, каналов распространения и каналов утечки информации (на примере конкретной фирмы).
- 25 Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах фирмы.
- 26 Основы технологии обработки и хранения конфиденциальных документов (по зарубежной литературе).
- 27 Назначение, виды, структура и технология функционирования системы защиты информации.
- 28 Поведение персонала и охрана фирмы в экстремальных ситуациях различных типов.
- 29 Аналитическая работа по выявлению каналов утечки информации фирмы.
- 30 Анализ функций секретаря-референта небольшой фирмы в области защиты информации.
- 31 Направления и методы защиты профессиональной тайны.
- 32 Направления и методы защиты служебной тайны.
- 33 Направления и методы защиты персональных данных о гражданах.
- 34 Методы защиты личной и семейной тайны.
- 35 Построение и функционирование защищенного документооборота.
- 36 Защита секретов в дореволюционной России.
- 37 Методика инструктирования и обучения персонала правилами защиты секретов фирмы.

Перечень контрольных вопросов

1. Определить место информационной безопасности в обеспечении системы общественной безопасности.
2. Дать определение информационной безопасности.
3. Назвать основные направления и задачи обеспечения информационной безопасности общества.
4. Назвать основные компоненты информационной безопасности автоматизированных информационных систем.
5. Охарактеризовать уровни реализации информационной безопасности.
6. Дать определение и классификацию информационных ресурсов.
7. Определить основные виды угроз информационным ресурсам.
8. Охарактеризовать особенности угроз конфиденциальной информации.
9. Проанализировать причины возникновения угроз утраты или утечки конфиденциальной информации.
10. Описать причины возникновения каналов несанкционированного доступа к информации.
11. Классифицировать виды каналов несанкционированного доступа к информации.
12. Описать характер действия организационных каналов несанкционированного

доступа к информации.

13. Охарактеризовать технические каналы несанкционированного доступа к информации.

14. Охарактеризовать легальные и нелегальные методы обеспечения действия каналов утечки информации.

15. Проанализировать особенности угроз автоматизированным информационным системам.

16. Дать классификацию удаленных атак.

17. Проанализировать основные направления правовой защиты информации.

18. Раскрыть содержание нормативных актов, защищающих право граждан на своевременное получение достоверной информации.

19. Изложить законный порядок реализации права гражданина на опровержение ложной информации о нем в средствах массовой информации.

20. Показать порядок защиты прав граждан на личную тайну и неприкосновенность частной жизни законодательством Российской Федерации о СМИ.

21. Определить объекты защиты авторских прав.

22. Назвать основные права автора в отношении его произведения.

23. Определить объекты интеллектуальной собственности, защищаемые патентным законодательством.

24. Охарактеризовать основные права патентообладателя в отношении его произведения (промышленного образца, полезной модели).

25. Дать определение государственной тайны и назвать грифы секретности.

26. Перечислить сведения, составляющие государственную тайну и сведения, которые не могут относиться к государственной тайне.

27. Изложить порядок отнесения сведений к государственной тайне и их засекречивания.

28. Раскрыть последовательность условия и формы допуска должностных лиц к государственной тайне.

29. Дать определение коммерческой тайны и перечислить сведения, которые не могут быть ее объектом.

30. Охарактеризовать порядок установления режима коммерческой тайны и основные права ее субъектов.

31. Назвать основные виды служебной тайны определенные законодательством Российской Федерации.

32. Изложить принципы и направления комплексного подхода к обеспечению информационной безопасности предприятия.

33. Назвать основные положения концепции информационной безопасности предприятия.

34. Изложить содержание регламента обеспечения информационной безопасности предприятия.

35. Определить основные методы и способы работы службы безопасности предприятия по защите конфиденциальной информации.

36. Определить критерии ценности информационных ресурсов и длительности сохранения ими этой характеристики.

37. Проанализировать содержание понятия разрешительной системы доступа персонала к конфиденциальным сведениям фирмы.

38. Обосновать критерии выделения конфиденциальных документов из общего потока поступающих документов.

39. Обосновать состав показателей учетной карточки (по выбору преподавателя) и правила их заполнения.

40. Проанализировать особенности контроля за исполнением конфиденциальных документов, его организационное и технологическое отличие от контроля открытых документов.

41. Классифицировать состав бумажных и технических носителей информации, применяемых для составления деловой (управленческой) и технической конфиденциальной документации.
42. Проанализировать особенности текста конфиденциального документа.
43. Регламентировать в виде фрагмента инструкции порядок работы исполнителей с конфиденциальными документами.
44. Проанализировать пути использования существующих средств копирования и тиражирования документов для изготовления экземпляров и копий конфиденциальных документов.
45. Сформулировать возможности, трудности и направления использования электронной почты для передачи конфиденциальных документов.
46. Составить фрагмент номенклатуры дел, содержащих конфиденциальные документы.
47. Проанализировать задачи защиты информации, которые должны быть решены при формировании и оформлении дел с конфиденциальными документами.
48. Классифицировать способы и средства физического уничтожения документов, изготовленных на носителях различных типов.
49. Проанализировать пути поиска документов и дел, не обнаруженных при проверке их наличия, дать рекомендации, повышающие эффективность поиска и предотвращающие утрату документов и дел.
50. Составить и проанализировать технологическую схему (цепочку) приема (перевода) лиц на работу, связанную с владением конфиденциальной информацией.
51. Составить и проанализировать технологическую схему (цепочку) увольнения сотрудников, владеющих конфиденциальной информацией.
52. Проанализировать виды угроз безопасности конфиденциальной информации фирмы при демонстрации на выставке новой продукции.
53. Составить схему каналов возможной утраты конфиденциальной информации, находящейся в компьютере, локальной сети, проанализировать степень опасности каждого канала.
54. Назвать основные элементы физической защиты территории и помещений предприятия.
55. Охарактеризовать способы и элементы программно-технической защиты информационных ресурсов.
56. Дать классификацию компьютерных вирусов.
57. Описать основные антивирусные программы.
58. Охарактеризовать основные способы криптографического преобразования данных.

6. Фонд оценочных средств для промежуточной аттестации по дисциплине (модулю).

6.1. Перечень компетенций выпускников образовательной программы с указанием результатов обучения (знаний, умений, владений), характеризующих этапы их формирования, описание показателей и критериев оценивания компетенций на различных этапах их формирования.

ОПК-1 способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ПК-3 способность владением навыками применения технических средств таможенного контроля и эксплуатации оборудования и приборов

ПК-25: способность организовывать сбор информации для управленческой деятельности, оценивать эффективность деятельности таможни (таможенного поста) и их структурных

подразделений, анализировать качество предоставляемых услуг (этап формирования компетенции – начальный)

ПК-32 владение навыками применения в таможенном деле информационных технологий и средств обеспечения их функционирования в целях информационного сопровождения профессиональной деятельности

ПК-34: способностью обеспечивать информацией в сфере таможенного дела государственные органы, организации и отдельных граждан

ПК-35: владением навыками использования электронных способов обмена информацией и средств их обеспечения, применяемых таможенными органами

Индикаторы компетенции	Оценка сформированности компетенций						
	Незачтено		Зачтено				
	плохо	неудовлетворительно	удовлетворительно	хорошо	очень хорошо	Отлично	превосходно
Полнота знаний	Отсутствие знаний теоретического материала. Невозможность оценить полноту знаний вследствие отказа обучающегося от ответа	Уровень знаний ниже минимальных требований. Имели место грубые ошибки.	Минимально допустимый уровень знаний. Допущено много негрубых ошибок.	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько несущественных ошибок	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок	Уровень знаний в объеме, превышающем программу подготовки
Наличие умений	Отсутствие минимальных умений. Невозможность оценить наличие умений вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки	Продemonстрированы основные умения. Решены типовые задачи с негрубыми ошибками. Выполнены все задания, но не в полном объеме	Продemonстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания, в полном объеме, но некоторые с недочетами	Продemonстрированы все основные умения. Решены все основные задачи. Выполнены все задания, в полном объеме, но некоторые с недочетами	Продemonстрированы все основные умения, решены все основные задачи с отдельными несущественными недочетами, выполнены все задания в полном объеме	Продemonстрированы все основные умения. Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов
Наличие навыков (владение опытом)	Отсутствие владения материалом. Невозможность оценить наличие навыков вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы базовые навыки. Имели место грубые ошибки	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	Продemonстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Продemonстрированы базовые навыки при решении стандартных задач без ошибок и недочетов	Продemonстрированы навыки при решении нестандартных задач без ошибок и недочетов	Продemonстрирован творческий подход к решению нестандартных задач
Мотивация (личностное отношение)	Полное отсутствие учебной активности и мотивации	Учебная активность и мотивация слабо выражены, готовность решать поставленные задачи качественно отсутствуют	Учебная активность и мотивация низкие, слабо выражены, стремление решать задачи качественно	Учебная активность и мотивация проявляются на среднем уровне, демонстрируется готовность выполнять поставленные задачи на среднем уровне качества	Учебная активность и мотивация проявляются на уровне выше среднего, демонстрируется готовность выполнять большинство поставленных задач на высоком уровне качества	Учебная активность и мотивация проявляются на высоком уровне, демонстрируется готовность выполнять все поставленные задачи на высоком уровне качества	Учебная активность и мотивация проявляются на очень высоком уровне, демонстрируется готовность выполнять дополнительные задачи на высоком уровне качества
Характеристика сформированности	Компетенция в не сформированном	Компетенция в полной мере	Сформированность компетенции	Сформированность компетенции	Сформированность компетенции	Сформированность компетенции	Сформированность компетенции превышает стандартные

ваниности компетенции	вана, отсутствуют знания, умения, навыки, необходимые для решения практических (профессиональных) задач. Требуется повторное обучение	не сформирована. Имеющихся знаний, умений, навыков недостаточно для решения практических (профессиональных) задач. Требуется повторное обучение	соответствует минимальным требованиям. Имеющихся знаний, умений, навыков в целом достаточно для решения практических (профессиональных) задач, но требуется дополнительная практика по большинству практических задач	в целом соответствует требованиям, но есть недочеты. Имеющихся знаний, умений, навыков и мотивации в целом достаточно для решения практических (профессиональных) задач, но требуется дополнительная практика по некоторым профессиональным задачам	в целом соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в целом достаточно для решения стандартных практических (профессиональных) задач	полностью соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в полной мере достаточно для решения сложных практических (профессиональных) задач.	требования. Имеющихся знаний, умений, навыков и мотивации в полной мере достаточно для применения творческого подхода к решению сложных практических (профессиональных) задач.
Уровень сформированности компетенций	Нулевой	Низкий	Ниже среднего	Средний	Выше среднего	Высокий	Очень высокий

6.2. Описание шкал оценивания результатов обучения по дисциплине

Итоговые результаты зачета оцениваются в соответствии с общепринятой в ННГУ методикой и критериями. Кроме знаний, навыков и умений, показанных студентами непосредственно на зачете, учитывается их текущая успеваемость - аттестация и работа в семестре.

Зачтено	<p>ставится, если:</p> <ul style="list-style-type: none"> – в ответе студента содержится глубокое знание программного материала, знание концептуально-понятийного аппарата всего курса, а также свидетельствует о способности увязывать теорию с практикой; – ответ студента свидетельствует о полном знании материала по программе, а также содержит в целом правильное, но не всегда точное и аргументированное изложение материала.
Не зачтено	ставится студенту, имеющему существенные пробелы в знании основного материала по программе, а также допустившему принципиальные ошибки при изложении материала.

6.3. Критерии и процедуры оценивания результатов обучения по дисциплине, характеризующих этапы формирования компетенций

По дисциплине «Информационная безопасность» предусмотрены разные формы контроля и оценки знаний, навыков и умений студентов. Текущий контроль успеваемости студентов осуществляется в ходе практических занятий, при выполнении и оценке самостоятельных заданий, по результатам тематического тестирования.

По итогам изучения дисциплины предусмотрен зачет с комплексной проверкой теоретических знаний, практических навыков и умений по применению информационных средств и технологий ИБ.

Теоретические знания оцениваются путем тестирования или на основании письменных или устных ответов студентов на поставленные теоретические вопросы из разных разделов и тем дисциплины.

Практические навыки определяются путем построения студентами на компьютере системы безопасности с использованием инструментальных средств ИТ-индустрии. При оценке задач учитываются полнота и правильность решения, выбор инструментария и соблюдение технологии решения, качество и время решения.

Критерии оценки тестов

«превосходно» - 96-100% правильных ответов;
 «отлично» – 86-95% правильных ответов;
 «очень хорошо» - 81-85% правильных ответов;
 «хорошо» – 66-80% правильных ответов;
 «удовлетворительно» – 56-65% правильных ответов.
 «неудовлетворительно» - 46-55% правильных ответов;
 «плохо» - 45% и меньше правильных ответов.

Описание шкалы оценивания для выполненных практических заданий

Оценка	Критерии оценивания
Превосходно	Задание выполнено в полном объеме (все поставленные задачи решены), ответ логичен и обоснован, студент отвечает четко и последовательно, показывает глубокое знание основного и дополнительного материала.
Отлично	Задание выполнено в полном объеме (все поставленные задачи решены), ответ логичен и обоснован, студент отвечает четко и последовательно, показывает глубокое знание основного материала
Очень хорошо	Задание выполнено в полном объеме (все поставленные задачи решены), ответ логичен и обоснован, студент отвечает четко и последовательно, показывает глубокое знание материала, допущено не более 2 неточностей не принципиального характера
Хорошо	Задание выполнено в полном объеме (все поставленные задачи решены), ответ логичен и обоснован, допущены неточности не принципиального характера, но студент показывает систему знаний по теме своими ответами на поставленные вопросы
Удовлетворительно	Задание выполнено не в полном объеме (решено более 50% поставленных задач), но студент допускает ошибки, нарушена последовательность ответа, но в целом раскрывает содержание основного материала
Неудовлетворительно	Задание выполнено не в полном объеме (решено менее 50% поставленных задач), студент дает неверную информацию при ответе на поставленные задачи, допускает грубые ошибки при толковании материала, демонстрирует незнание основных терминов и понятий.
Плохо	Задание не выполнено, студент демонстрирует полное незнание материала

Описание шкалы оценивания для выполненных разноуровневых заданий и задач

Оценка	Критерии оценивания
Превосходно	Студент демонстрирует полные и глубокие знания теоретического материала курса, уверенно применяет полученные знания на практике, приобрёл умение быстро ориентироваться в содержании материала, понимает и умеет логично и последовательно разъяснить смысл

	своего ответа, доказать необходимость использования тех или иных теоретических положений, аргументированно и корректно отстаивает свою позицию, во всех случаях способен предложить альтернативные варианты решения проблемы.
Отлично	Студент демонстрирует полные и глубокие знания теоретического материала курса, уверенно применяет полученные знания на практике, приобрёл умение быстро ориентироваться в содержании материала, понимает и умеет логично и последовательно разъяснить смысл своего ответа, доказать необходимость использования тех или иных теоретических положений, аргументированно и корректно отстаивает свою позицию, в более чем 50% случаев способен предложить альтернативные варианты решения проблемы.
Очень хорошо	Студент демонстрирует знание теоретического материала, но применение теоретических положений на практике вызывает несущественные затруднения, связанные с аргументацией своей позиции. Обучающийся в полной мере понимает суть проблемы. Основные требования к заданию выполнены. В более чем 50% случаев способен предложить альтернативные варианты решения проблемы.
Хорошо	Студент демонстрирует знание теоретического материала, но применение теоретических положений на практике вызывает некоторые затруднения, связанные с аргументацией своей позиции. Обучающийся в полной мере понимает суть проблемы. Основные требования к заданию выполнены. В принципе способен предложить альтернативные варианты решения проблемы.
Удовлетворительно	Студент обладает знанием необходимого минимума теоретического материала, способен дать ответ не менее, чем на 50% поставленных заданий, но не способен аргументированно излагать свою позицию, не видит альтернативных вариантов разрешения проблемной ситуации, не может последовательно изложить суть решения.
Неудовлетворительно	Студент не обладает знанием требуемым объёмом знаний теоретического материала, способен дать ответ менее, чем на 50% поставленных заданий, не способен аргументированно излагать свою позицию, не видит альтернативных вариантов разрешения проблемной ситуации, не может последовательно изложить суть решения.
Плохо	Студент не обладает требуемым объёмом знаний теоретического материала и не может решить практическое задание.

6.4. Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения, характеризующих этапы формирования компетенций и (или) для итогового контроля сформированности компетенции.

Примеры тестовых заданий

На каждый вопрос предложено три варианта ответа. Выберите один правильный и отметьте его ✓.

1. Третьим этапом построения системы защиты является:

- планирование;
- реализация;
- анализ.

2. «Люком» называется..?

- использование после окончания работы части данных, оставшиеся в памяти;
- передача сообщений в сети от имени другого пользователя;
- неописанная в документации на программный продукт возможность работы с ним.

3. Правовое обеспечение информационной безопасности - это..?
- нормативные документы по ИБ, требования которых являются обязательными в рамках сферы действия каждого подразделения;
 - документированные сведения, лежащие в основе решения задач, обеспечивающих функционирование системы;
 - широкое использование технических средств защиты информации.
4. К активным угрозам относятся:
- попытка получения информации, циркулирующей в каналах связи, посредством их прослушивания;
 - разрушение или радиоэлектронное подавление линий связи, вывод из строя ПЭВМ или ее операционной системы;
 - копирование информации.
5. Какого подхода к обеспечению безопасности информации не существует?
- комплексный;
 - фрагментарный;
 - теоретический.
6. Типовыми путями несанкционированного доступа к информации, являются:
- дистанционное фотографирование;
 - выход из строя ПЭВМ;
 - ураганы.
7. Первым этапом построения системы защиты является:
- анализ;
 - планирование;
 - сопровождение.
8. «Троянский конь»- это ...?
- способ, состоящий в тайном введении в чужую программу вредоносных команд;
 - встраивание в программу набора команд, срабатываемых при определенных условиях;
 - проникновение в компьютерную систему злоумышленников, выдающих себя за законного пользователя.
9. В политике безопасности основным принципом является усиление самого слабого звена?
- нет;
 - да;
 - отчасти.
10. Криптографические средства - это..?
- регламентация правил использования, обработки и передачи информации ограниченного доступа;
 - средства защиты с помощью преобразования информации (шифрование);
 - средства, в которых программные и аппаратные части полностью взаимосвязаны.
11. Шифрование с симметричным ключом предполагает, что..?
- используются два разных ключа;
 - оба ключа одинаковы;
 - невозможно отказаться от авторства.
12. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети предусмотрено в ..?
- ст. 272 УК РФ;
 - ст. 273 УК РФ;
 - ст. 274 УК РФ.
13. Информационная война – это...
- А. злословие в адрес другого человека;
- Б. информационное противоборство с целью нанесения ущерба важным структурам противника, подрыв его политической и социальной систем, а также дестабилизации общества и государства противника;

В. акт применения информационного оружия.

14. Информационная безопасность – это...

А. невозможность нанесения вреда свойствам объектам безопасности, обуславливаемым информацией и информационной инфраструктурой (защищенность от угроз);

Б. предотвращение зла наносимого государственным структурам;

В. проведение природоохранных мероприятий.

15. К понятию информационной безопасности НЕ относятся:

А. природоохранные мероприятия;

Б. надежность работы компьютера;

В. сохранность ценных данных.

16. К объектам информационной безопасности на предприятии НЕ относятся:

А. информационные ресурсы;

Б. средства вычислительной и организационной техники;

В. Конституция России.

17. Обеспечение безопасности информации – это...

А. одноразовое мероприятие;

Б. комплексное использование всего арсенала имеющихся средств защиты;

В. разработка каждой службой плановых мер по защите информации.

6.5. Методические материалы, определяющие процедуры оценивания.

Положение «О проведении текущего контроля успеваемости и промежуточной аттестации обучающихся в ННГУ», утвержденное приказом ректора ННГУ № 630-ОД от 29.12.2017 г.,

Положение о фонде оценочных средств, утвержденное приказом ректора ННГУ от 10.06.2015 №247-ОД.

7. Учебно-методическое обеспечение дисциплины

Основная литература

1. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — М. : Издательство Юрайт, 2017. — 321 с. — (Серия : Университеты России). — ISBN 978-5-534-00258-4. — Режим доступа : www.biblio-online.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7

Дополнительная литература

1. Учебное пособие «Информационная безопасность» / Ясенев В.Н., Дорожкин А.В., Сочков А.Л., Ясенев О.В. Нижний Новгород: Нижегородский госуниверситет им. Н.И.Лобачевского, 2017. - 198с Режим доступа: <http://znanium.com>

2. Одинцов, Б. Е. Информационные системы управления эффективностью бизнеса : учебник и практикум для бакалавриата и магистратуры / Б. Е. Одинцов. — М. : Издательство Юрайт, 2017. — 206 с. — (Серия : Бакалавр и магистр. Модуль.). — ISBN 978-5-534-01052-7. — Режим доступа : www.biblio-online.ru/book/A776D72A-816A-4037-A427-23F71AF28852

Программное обеспечение:

1) MSWindows 7 (лицензия на ГОУ ВПО ННГУ им. Лобачевского, идентификатор 47276400).

2) MicrosoftOffice 2007 Профессиональный + (лицензия на ГОУ ВПО ННГУ им. Лобачевского, идентификатор 47729513).

3) KasperskyEndpointSecurity 10 forWindows.

8. Материально-техническое обеспечение дисциплины (модуля)

Для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а для самостоятельной работы студентов используются специальные помещения, укомплектованные специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

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

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду ННГУ.

Программа составлена в соответствии с требованиями ОС ННГУ по специальности 38.05.02 «Таможенное дело», специализация «Таможенные операции и таможенный контроль».

Автор программы:

Зав.каф. ИС в ФКС к.э.н., профессор _____ Ясенов В.Н.

Рецензент:

Директор ООО «Акватория развлечений»

_____ С.А. Микаелян

Зав.каф. ИС в ФКС к.э.н., профессор _____ Ясенов В.Н.

Программа одобрена на заседании методической комиссии Института экономики и предпринимательства от «26» марта 2020 года, протокол № 3.