МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «РОССИЙСКИЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ Г.В. ПЛЕХАНОВА»

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ ЭКОНОМИКИ И ТОРГОВЛИ ИМЕНИ МИХАИЛА ТУГАН-БАРАНОВСКОГО»

УТВЕРЖДАЮ
Проректор по учебно-методической работе _____ Л.В. Крылова
«28» 02 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О. 15 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Специальность	**38.05.02 Таможенное дело**
Специализация	**Таможенные платежи и валютное регулирование**
Уровень высшего образования:	**Специалитет**

Москва – Донецк – 2024 г.

Рабочая программа учебной дисциплины «Информационная безопасность» для обучающихся по специальности 38.05.02 Таможенное дело, программа специалитета, специализация Таможенные платежи и валютное регулирование, разработанная в соответствии с учебным планом, утвержденным Ученым советом ФГБОУ ВО «ДОННУЭТ»:

- в 2023 г. - для очной формы обучения.

Разработчик: Пальчикова Н.С., старший преподаватель кафедры информационных систем и технологий управления

Рабочая программа утверждена на заседании кафедры информационных систем и технологий управления

Протокол от «12» февраля 2024 года №19

Зав. кафедрой

КАФЕДРА ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ УПРАВЛЕНИЯ

_____ В.О. Бессарабов
(подпись) (инициалы, фамилия)

СОГЛАСОВАНО
Декан факультета таможенного дела

ФАКУЛЬТЕТ ТАМОЖЕННОГО ДЕЛА

_____ А.В. Шершнева
(подпись) (инициалы, фамилия)

Дата «_____» _____ 2024 года

ОДОБРЕНО
Учебно-методическим советом ФГБОУ ВО «ДОННУЭТ»
Протокол от «27» 02 2024 года № 7
Председатель_____ Л.В. Крылова
(подпись) (инициалы, фамилия)

1. ОПИСАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

<table>
<tr><td rowspan="2">Наименование показателя</td><td rowspan="2">Наименование укрупненной группы направлений подготовки / специальностей, направление подготовки / специальность, профиль / магистерская программа / специализация, программа высшего образования</td><td colspan="2">Характеристика учебной дисциплины</td></tr>
<tr><td>очная форма обучения</td><td>заочная форма обучения</td></tr>
<tr><td rowspan="2">Количество зачетных единиц – 4</td><td>Укрупненная группа специальностей
38.00.00 Экономика и управление</td><td colspan="2" rowspan="2">Обязательная часть</td></tr>
<tr><td>Специальность
38.05.02 Таможенное дело</td></tr>
<tr><td>Модулей – 1</td><td rowspan="6">Специализация: Таможенные платежи и валютное регулирование</td><td colspan="2">Год подготовки</td></tr>
<tr><td>Смысловых модулей – 3</td><td>1й</td><td></td></tr>
<tr><td rowspan="5">Общее количество часов – 144</td><td colspan="2">Семестр</td></tr>
<tr><td>1-й</td><td></td></tr>
<tr><td colspan="2">Лекции</td></tr>
<tr><td>14 час.</td><td></td></tr>
<tr><td rowspan="11">Количество часов в неделю для очной формы обучения:

аудиторных – 1,8;
самостоятельной работы обучающегося – 4</td><td rowspan="11">Программа высшего образования – программа специалитета</td><td colspan="2">Практические, семинарские занятия</td></tr>
<tr><td>14 час.</td><td></td></tr>
<tr><td colspan="2">Лабораторные занятия</td></tr>
<tr><td>6 час.</td><td></td></tr>
<tr><td colspan="2">Самостоятельная работа</td></tr>
<tr><td>74 час.</td><td></td></tr>
<tr><td colspan="2">Индивидуальные задания*:</td></tr>
<tr><td>ТМК 3</td><td>-</td></tr>
<tr><td colspan="2">Форма промежуточной аттестации:
(зачет с оценкой, экзамен)</td></tr>
<tr><td>экзамен</td><td></td></tr>
</table>

* для очной формы обучения указывается количество проводимых текущих модульных контролей (например, 2ТМК), при наличии – курсовая работа/проект (КР/КП)

для заочной формы обучения указывается, при наличии, аудиторная письменная работа/контрольная работа (АПР), курсовая работа/проект (КР/КП)

Соотношение количества часов аудиторных занятий и самостоятельной работы составляет:
для очной формы обучения – 34/74

1. ЦЕЛЬ И ЗАДАЧИ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цель учебной дисциплины: формирование у студентов знаний и представлений о смысле, целях и задачах информационной защиты, характерных свойствах защищаемой информации, основных информационных угрозах, существующих (действующих) направлениях защиты и возможностях построения моделей, стратегий, методов и правил информационной защиты.

Задачи учебной дисциплины: ознакомление с основными уязвимостями экономических информационных систем и угрозами информационной безопасности; правилами их выявления, анализа и определение требований к различным уровням обеспечения информационной безопасности в корпоративных сетях и в глобальной сети Internet.

3. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Учебная дисциплина Б 1.О.15 «Информационная безопасность» относится к обязательной части, формируемой участниками образовательных отношений ОПОП ВО.

Знания, навыки и умения, приобретенные обучающимся при успешном освоении курса, послужат необходимой мировоззренческой и методологической информационной базой при подготовке научно-исследовательской работы, выпускной квалификационной работы, в дальнейшей педагогической практике.

4. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

В результате освоения учебной дисциплины обучающийся должен обладать такими компетенциями:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.2 Разрабатывает варианты решения проблемной ситуации на основе критического анализа доступных источников информации

В результате изучения учебной дисциплины обучающийся должен:

знать: базовый понятийный аппарат в области информационной безопасности; принципы и общие методы обеспечения информационной безопасности; критерии, условия и принципы отнесения информации к защищаемой; принципы и методы обработки конфиденциальных документов; методы и приемы защиты документированной информации от несанкционированного доступа;

уметь: практически выполнять технологические операции по защите и обработке конфиденциальных документов; разрабатывать политику предприятия в соответствии со стандартами безопасности; применить и настроить различные средства защиты информации; оценивать качество информационных ресурсов.

владеть: методами и формами защиты информации; технологией составления конфиденциальных документов; практическими навыками применения средств защиты информации при решении профессиональных задач, приёмами социальной адаптации информационных ресурсов и информационных технологий.

5. ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Смысловой модуль 1. Информационная безопасность в экономических информационных системах.

Тема 1. Введение в информационную безопасность. Модели информационной безопасности.

Тема 2. Выявление возможных нарушений и атак в экономических информационных системах (ЭИС).

Смысловой модуль 2. Инструменты защиты информации в экономических информационных системах.

Тема 3. Противодействие вредоносным программам в ЭИС.

Тема 4. Применение криптографических систем шифрования данных.

Тема 5. Методы защиты информации в корпоративных вычислительных сетях (Интранет).

Тема 6. Методы защиты информации в глобальной сети Интернет.

Смысловой модуль 3. Проверка состояния информационной безопасности в экономических информационных системах.

Тема 7. Аудит информационной безопасности.

Тема 8. Анализ информационных рисков.

6. СТРУКТУРА УЧЕБНОЙ ДИСЦИПЛИНЫ

Название смысловых модулей и тем	Количество часов											
	очная форма обучения						заочная форма обучения					
	всего	в том числе					всего	в том числе				
		л[1]	п[2]	лаб[3]	инд[4]	СР[5]		л	п	лаб	инд	СР
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
МОДУЛЬ 1. Информационная безопасность.												
Смысловой модуль 1. Информационная безопасность в экономических информационных системах.												
Тема 1. Введение в информационную безопасность. Модели информационной безопасности.	11	1	1			9						
Тема 2. Выявление возможных нарушений и атак в экономических информационных системах (ЭИС).	12	1	1	1		9						
Итого по смысловому модулю 1	**23**	**2**	**2**	**1**		**18**						
Смысловой модуль 2. Инструменты защиты информации в экономических информационных системах.												
Тема 3. Противодействие вредоносным программам в ЭИС.	14	2	2	1		9						
Тема 4. Применение криптографических систем шифрования данных.	14	2	2			10						
Тема 5. Методы защиты информации в	14	2	2	1		10						

Название смысловых модулей и тем	Количество часов											
	очная форма обучения						заочная форма обучения					
	всего	в том числе					всего	в том числе				
		л[1]	п[2]	лаб[3]	инд[4]	СР[5]		л	п	лаб	инд	СР
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
корпоративных вычислительных сетях (Интранет).												
Тема 6. Методы защиты информации в глобальной сети Интернет.	14	2	2	1		9						
Итого по смысловому модулю 2	**56**	**8**	**8**	**3**		**38**						
Смысловой модуль 3. Проверка состояния информационной безопасности в экономических информационных системах.												
Тема 7. Аудит информационной безопасности.	14	2	2	1		9						
Тема 8. Анализ информационных рисков.	14	2	2	1		9						
Итого по смысловому модулю 3	**28**	**4**	**4**	**2**		**18**						
Всего часов	**108**	**14**	**14**	**6**		**74**						
Всего по смысловым модулям	**108**											
Катт												
СРэк	**33**											
ИК												
КЭ	**1**											
Каттэк	**2**											
Контроль												
Всего часов	**144**	**14**	**14**	**6**		**74**						

Примечания: 1. л – лекции;
2. п – практические (семинарские) занятия;
3. лаб – лабораторные занятия;
4. инд – индивидуальные занятия;
5. СР – самостоятельная работа.

7. ТЕМЫ СЕМИНАРСКИХ И ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Номер п/п	Название темы	Количество часов	
		очная форма	заочная форма
1	Введение в информационную безопасность. Модели информационной безопасности.	1	
2	Выявление возможных нарушений и атак в экономических информационных системах (ЭИС).	1	
3	Противодействие вредоносным программам в ЭИС.	2	
4	Применение криптографических систем	2	

	шифрования данных.		
5	Методы защиты информации в корпоративных вычислительных сетях (Интранет).	2	
6	Методы защиты информации в глобальной сети Интернет.	2	
7	Аудит информационной безопасности.	2	
8	Анализ информационных рисков.	2	
Всего:		14	

8. ТЕМЫ ЛАБОРАТОРНЫХ ЗАНЯТИЙ – не предусмотрены

№ п/п	Название темы	Количество часов	
		очная форма	заочная/очно-заочная форма
1	Введение в информационную безопасность. Модели информационной безопасности.		
2	Выявление возможных нарушений и атак в экономических информационных системах (ЭИС).	1	
3	Противодействие вредоносным программам в ЭИС.	1	
4	Применение криптографических систем шифрования данных.		
5	Методы защиты информации в корпоративных вычислительных сетях (Интранет).	1	
6	Методы защиты информации в глобальной сети Интернет.	1	
7	Аудит информационной безопасности.	1	
8	Анализ информационных рисков.	1	
Всего:		6	

9. САМОСТОЯТЕЛЬНАЯ РАБОТА

Номер п/п	Название темы	Количество часов	
		очная форма	заочная форма
1	Сеть Интернет как инструмент маркетинга.	9	
2	Разработка стратегии продвижения в сети Интернет	9	
3	Информационная безопасность в профессиональной деятельности.	5	
4	Методы сбора и анализа маркетинговой информации.	10	
5	Методы прогнозирования экономических показателей.	10	
6	Обзор пакетов прикладных программ для маркетинговой и рекламной деятельности.	5	
7	Аудит информационной безопасности.	9	
8	Анализ информационных рисков.	9	
Всего:		74	

10. ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

В ходе реализации учебной дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

1) для слепых и слабовидящих:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
- письменные задания оформляются увеличенным шрифтом…

2) для глухих и слабослышащих:

- лекции оформляются в виде электронного документа;
- письменные задания выполняются на компьютере в письменной форме;
- экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

3) для лиц с нарушениями опорно-двигательного аппарата:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере…

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

1) для слепых и слабовидящих:
   - в печатной форме увеличенным шрифтом;
   - в форме электронного документа;
2) для глухих и слабослышащих:
   - в печатной форме;
   - в форме электронного документа.
3) для обучающихся с нарушениями опорно-двигательного аппарата:
   - в печатной форме;
   - в форме электронного документа.

11. ИНДИВИДУАЛЬНЫЕ ЗАДАНИЯ

Примеры тестовых заданий для проведения текущего модульного контроля (ТМК)

Примеры тестовых заданий по смысловому модулю 1

1. Информация - это

А) это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

Б) совокупность некоторых знаков, символов, сигналов;

В) отдельные документы и отдельные массивы документов.

2. Защищаемая информация - это

А) совокупность технических средств и программного обеспечения, а также методов обработки информации и действий персонала;

Б) информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственниками информации;

В) это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

3. Система обработки информации - это

А) совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов;

Б) отдельные документы и отдельные массивы документов, документы и массивы документов, содержащиеся в информационных системах;

В) совокупность технических средств и программного обеспечения, а также методов обработки информации и действий персонала, необходимых для выполнения автоматизированной обработки информации.

4. Объект информатизации - это

А) совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов;

Б) информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственниками информации;

В) совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

5. Выделяются следующие направления защиты информации:

А) правовая защита информации;

Б) техническая защита информации;

В) криптографическая защита информации;

Г) физическая защита информации;

Д) математическая защита информации.

6. Средство защиты информации -это

А) техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации;

Б) средства контроля эффективности защиты информации;

В) средства физической защиты информации;

Г) криптографические средства защиты информации.

7. Этапы развития информационной безопасности:

А) 1816, 1816, 1935, 1946, 1965, 1973, 1985;

Б) 1745,1863,1935,1965,1970,1973, 1985;

В) 1815,1817,1934,1945,1966,1974,1989;

Г) 1812,1816,1931,1941,1960,1971,1981.

8. Основными задачами системы ИБ являются:

А) своевременное выявление и устранение угроз безопасности и ресурсам, причин и условий, способствующих нанесению финансового, материального и морального ущерба интересам субъектов информационных отношений;

Б) актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения;

В) создание механизма и условий оперативного реагирования на угрозы безопасности и проявлению негативных тенденций в функционировании предприятия;

Г) эффективное пресечение посягательств на ресурсы и угроз персоналу на основе правовых, организационных и инженерно-технических мер и средств обеспечения

безопасности;

Д) создание условий для максимально возможного возмещения и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния последствий нарушения безопасности на достижение целей организации.

9. Основу мандатной политики безопасности составляет мандатное управление доступом, которое подразумевает, что:

А) все субъекты и объекты должны быть идентифицированы, задан линейно упорядоченный набор меток секретности;

Б) каждому объекту системы присвоена метка секретности, определяющая ценность содержащейся в нем информации - его уровень секретности;

В) каждому субъекту системы присвоена метка секретности, определяющая уровень доверия к нему - его уровень доступа;

Г) решение о разрешении доступа субъекта к объекту принимается исходя из типа доступа и сравнения метки субъекта и объекта.

10. Уязвимость - это

А) это присущие объекту ЭИС причины, приводящие к нарушению безопасности информации на конкретном объекте и обусловленные недостатками процесса функционирования объекта ИС, свойствами архитектуры ЭИС, протоколами обмена и интерфейсами, применяемым программным обеспечением и аппаратной платформы, условиями эксплуатации, невнимательностью сотрудников

Б) это возможные действия реализации угрозы при взаимодействии источника угрозы через имеющиеся уязвимости

В) это потенциальные антропогенные, техногенные и стихийные угрозы безопасности

Примеры тестовых заданий по смысловому модулю 2

1. Асинхронная атака - это

А) используется как для анализа процессов, в которые преступники хотят вмешаться, так и для планирования методов совершения преступления

состоит в смешивании и одновременном выполнении компьютерной системой команд двух или нескольких пользователей;

Б) разновидность логической бомбы, которая срабатывает при достижении определенного момента времени;

В) использование компьютерных систем или сетей для хранения, обмена, распространения или перемещения информации конфиденциального характера.

2. К интересующим нарушителя персональным данным пользователя атакуемого компьютера относятся:

А) хранящиеся в памяти компьютера документы и другие данные пользователя;

Б) имена учетных записей и пароли для доступа к различным сетевым ресурсам (системам электронных денег и платежей, Интернет-аукционам, Интернет-пейджерам, электронной почте, Интернет-сайтам и форумам, онлайн-играм);

В) адреса электронной почты других пользователей, 1Р-адреса других компьютеров сети.

3. После получения управления код вируса выполняет следующую последовательность действий:

А) заражение других файлов (комбинированные вирусы) и системных областей дисковой памяти;

Б) установка в оперативной памяти собственных резидентных модулей (резидентные вирусы);

В) выполнение других действий, зависящих от реализуемого вирусом алгоритма;

Г) продолжение обычной процедуры открытия файла (например, передача управления исходному коду зараженной программы).

4. При запуске зараженного файла управление получает код вируса, который:

А) устанавливает в оперативной памяти свой резидентный модуль, который в дальнейшем

будет перехватывать все обращения к зараженному диску;

Б) загружает исходный программный файл и передает ему управление;

В) код программы реального режима процессора, которая получает управление при попытке запуска приложения Windows в среде операционной системы MS-DOS.

5. Простейший макровирус в документе MicrosoftWord заражает остальные файлы документов следующим образом:

А) при открытии зараженного документа управление получает содержащийся в нем макрос с кодом вируса;

Б) вирус помещает в файл шаблонов normal.dot другие макросы со своим кодом (например, FileOpen, FileSaveAs и FileSave);

В) вирус устанавливает в реестре Windows и (или) в инициализационном файле MicrosoftWord соответствующий флаг о произведенном заражении;

Г) при последующем запуске MicrosoftWord первым открываемым файлом фактически является уже зараженный файл шаблонов normal.dot, что позволяет коду вируса автоматически получать управление, а заражение других файлов документов может происходить при их сохранении с помощью стандартных команд MicrosoftWord.

6. Программной закладкой называют

А) внешнюю или внутреннюю по отношению к атакуемой компьютерной системе программу, обладающую определенными разрушительными функциями по отношению к этой системе;

Б) осуществление различных несанкционированных пользователем действий (сбор конфиденциальной информации и ее передачу нарушителю, разрушение или намеренную модификацию информации пользователя, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях ("троянские" программы или просто "троянцы");

В)уничтожение или внесение изменений в функционирование программного обеспечение КС, уничтожение или изменение обрабатываемых в ней данных после выполнения некоторого условия или получения некоторого сообщения извне КС ("логические бомбы");

Г) перехват паролей пользователей КС с помощью имитации приглашения к его вводу или перехвата всего ввода пользователей с клавиатуры.

7. Криптографией принято называть

А) науку о математических методах обеспечения конфиденциальности и аутентичности (целостности и подлинности) информации;

Б) способ скрытой передачи сообщений без сокрытия самого факта их передачи;

В) тайнопись.

8. Временная сложность - это

А) объем памяти, необходимой для хранения полученных в ходе работы данных, как функция от размера задачи;

Б) это время, затрачиваемое алгоритмом для решения задачи, рассматриваемое как функция от размера задачи

В) стойкость шифра к раскрытию методами криптоанализа

9. По типу преобразований шифры можно разделить на следующие группы:

А) шифры замены (подстановки);

Б) шифры перестановки;

В) шифры гаммирования;

Г) шифры на основе математических преобразований;

Д) шифры на основе аналитических преобразований.

10. По типу использования ключей шифры делятся на:

А) симметричные;

Б) асимметричные;

В) использующие для шифрования и расшифровывания два различных ключа;

Г) блочные;

Д) потоковые.

Примеры тестовых заданий по смысловому модулю 3

1. Аудит информационной безопасности предприятия – это

А) сбор и накопление информации о событиях, происходящих в информационной системе;

Б) анализ накопленной информации, проводимый оперативно, в реальном времени или периодически;

В) процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности организации в соответствии с определенными критериями, стандартами и показателями.

2. Реализация протоколирования и аудита решает следующие задачи:

А) выявление нештатных ситуаций;

Б) обеспечение подотчетности пользователей и администраторов;

В) обеспечение возможности реконструкции последовательности событий;

Г) обнаружение попыток нарушений информационной безопасности;

Д) предоставление информации для выявления и анализа проблем.

3. Под подозрительной активностью понимается

А) активность, не соответствующая политике безопасности

поведение пользователя или компонента информационной системы, являющееся злоумышленным;

Б) совокупность условий, при выполнении которых атака считается имеющей место, что вызывает заранее определенную реакцию;

В) действия, выполняемые в рамках имеющихся полномочий, но нарушающие политику безопасности.

4. Сигнатура атаки - это

А) совокупность условий, при выполнении которых атака считается имеющей место, что вызывает заранее определенную реакцию;

Б) зависимость от других средств безопасности;

В) описание изменений, внесенных в базы данных защиты;

Г) имена затронутых объектов.

5. Анализ информационных рисков - это

А) анализ осуществляющийся при помощи различных инструментов и методов формирования процессов защиты информации;

Б) это процесс совокупного оценивания степени защиты информационной системы с определением количественных;

В)автоматизация управления рисками, оптимизация финансовых расходов на управление, оптимизация времени на сопровождение систем безопасности компании, поддержка непрерывности бизнеса.

6. Наиболее известным подходом к количественному расчету информационных рисков является

А) AssetValue;

Б) ExposureFactor;

В) CRAMM;

Г) AnnualRateofOccurrence.

12. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ ЗНАНИЙ ОБУЧАЮЩИХСЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Оценочные средства детализируются по видам работ в оценочных материалах по учебной дисциплине, которые утверждаются на заседании кафедры.

Система оценивания по учебной дисциплине по очной форме обучения*

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль:		
- тестирование (темы смысловых модулей 1,2,3)	10	30
- практическая работа (тема 1,2,3,4)	5	20
- практическая работа (тема 5)	5	5
- практическая работа (тема 8)	5	5
Промежуточная аттестация	*Экзамен*	*60*
Итого за семестр	*100*	

* в соответствии с утвержденными оценочными материалами по учебной дисциплине

Вопросы для подготовки к промежуточной аттестации обучающихся (экзамен)

1. Понятие информационной безопасности.
2. Модели информационной безопасности
3. Выявление возможных нарушений и атак в экономических информационных системах.
4. Анализ угроз информационной безопасности.
5. Классификация угроз информационной безопасности
6. Уязвимости ЭИС
7. Классификация компьютерных преступлений
8. Противодействие вредоносным программам в ЭИС.
9. Вредоносные программы и их классификация
10. Принцип работы вредоносных программ
11. Вирусы и их классификация
12. Макровирусы
13. Программные закладки
14. Применение криптографических систем шифрования данных.
15. Основные понятия. Классификация шифров
16. Требования криптографических систем защиты
17. Симметричные криптосистемы
18. Системы с открытым ключом
19. Управление ключами
20. Реализация криптографических методов
21. Методы защиты информации в корпоративных вычислительных сетях.
22. Идентификация и аутентификация.
23. Способы атаки на пароль.
24. Использование токенов.
25. Управление доступом.
26. Методы защиты информации в глобальной сети Интернет
27. Средства защиты сети
28. Межсетевые экраны
29. Виртуальные частные сети (VPN)
30. Системы обнаружения вторжений (IDS)
31. Аудит информационной безопасности.
32. Протоколирование и аудит
33. Активный аудит

34. Функциональные компоненты и архитектура активного аудита
35. Анализ информационных рисков.
36. Понятие информационного риска
37. Методики анализа, оценки и управления рисками информационной безопасности
38. Методы оценки рисков информационной безопасности

13. РАСПРЕДЕЛЕНИЕ БАЛЛОВ, КОТОРЫЕ ПОЛУЧАЮТ ОБУЧАЮЩИЕСЯ

Максимальное количество баллов за текущий контроль и самостоятельную работу								**Максимальная сумма баллов**		
Смысловой модуль № 1		**Смысловой модуль № 2**				**Смысловой модуль № 3**		**Текущий контроль**	**Экзамен**	**Все виды учебной деятельности**
T1[1]	T2	T3	T4	T5	T6	T7	T8	40	60	100
5	5	5	5	5	5	5	5			

Примечание. T1, T2, ... T12 – номера тем соответствующих смысловых модулей

Соответствие государственной шкалы оценивания академической успеваемости

Сумма баллов за все виды учебной деятельности	**По государственной шкале**	**Определение**
90-100	«Отлично» (5)	отлично – отличное выполнение с незначительным количеством неточностей
80-89	«Хорошо» (4)	хорошо – в целом правильно выполненная работа с незначительным количеством ошибок (до 10 %)
75-79		хорошо – в целом правильно выполненная работа с незначительным количеством ошибок (до 15 %)
70-74	«Удовлетворительно» (3)	удовлетворительно – неплохо, но со значительным количеством недостатков
60-69		удовлетворительно – выполнение удовлетворяет минимальные критерии
35-59	«Неудовлетворительно» (2)	неудовлетворительно – с возможностью повторной аттестации
0-34		неудовлетворительно – с обязательным повторным изучением дисциплины (выставляется комиссией)

15. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

1. Графов, А. А. Информационная безопасность в системе экономической безопасности [Электронный ресурс] : учеб. пособие / А. А. Графов, В. А. Мордовец ; М-во образования и науки РФ, ФГБОУ ВО "Санкт-Петербург. гос. экон. ун-т", Каф. экон. безопасности . — СПб.: Изд-во СПбГЭУ, 2018. — Локал. компьютер сеть НБ ДонНУЭТ .

2. Груздева, Л. М. Информационная безопасность [Электронный ресурс]: учебно-методическое пособие / Л. М. Груздева. — Москва: Издательство "Академия Естествознания", 2020. — 121 с.

3. Информационная безопасность [Электронный ресурс]: учебное пособие / В. И. Лойко [и др.] . — Краснодар: КубГАУ, 2020. — Локальная компьютерная сеть НБ ДонНУЭТ.

Дополнительная литература:

1. Панфилова, О. А. Информационная безопасность и защита информации [Электронный ресурс] : учебное пособие для направления подготовки 40.03.01 – Юриспруденция, специальности 40.05.02 – Правоохранительная деятельность, специальности 37.05.02 – Психология служебной деятельности, очной и заочной форм обучения / О. А. Панфилова, А. Н. Наимов ; Федеральная служба исполнения наказаний, Вологодский институт права и экономики . — Вологда: ВИПЭ ФСИН России, 2018. — Локал. компьютер сеть НБ ДонНУЭТ. — 978-5-94991-428-1.

2. Соколовская, С. А. Информационные технологии и информационная безопасность в государственном управлении [Электронный ресурс]: учебное пособие / С. А. Соколовская; Министерство науки и высшего образования РФ, Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный экономический университет», Кафедра вычислительных систем и программирования. — Санкт-Петербург: СПбГЭУ, 2019. — Локал. компьютер сеть НБ ДонНУЭТ . — 978-5-7310-4685-5.

Учебно-методические издания:

1. Информационная безопасность [электронный ресурс]: метод. реком. для организации самостоятельной работы обуч. специальности 38.05.02 Таможенное дело (Специализация: Таможенные платежи и валютное регулирование) очной формы обучения / М-во образования и науки РФ., Федеральное государственное бюджетное образовательное учреждение высшего образования «Донецкий национальный университет экономики и торговли имени Михаила Туган-Барановского», каф. информац. систем и технологий упр. Пальчикова Н.С. – Донецк: [ФГБОУ ВО «ДОННУЭТ»], 2023 – 23 с.

2. Информационная безопасность [электронный ресурс]: метод. указ. для проведения практ. занятий для обуч. специальности 38.05.02 Таможенное дело (Специализация: Таможенные платежи и валютное регулирование) очной формы обучения / М-во образования и науки РФ., Федеральное государственное бюджетное образовательное учреждение высшего образования «Донецкий национальный университет экономики и торговли имени Михаила Туган-Барановского», каф. информац. систем и технологий упр. Пальчикова Н.С., Глотова Д.В. – Донецк: [ФГБОУ ВО «ДОННУЭТ»], 2023 – 41 с.

3. информационная безопасность: конспект лекций для обучающихся Специальности 38.05.02 Таможенное дело (Специализация: Таможенные платежи и валютное регулирование), очной формы обучения / Н.С. Пальчикова; Министерство образования и науки Российской Федерации, Донецкий национальный университет экономики и торговли имени Михаила Туган-Барановского, Кафедра информационных систем и технологий управления. – Донецк: ДОННУЭТ , 2024 - 7 4 с. - Текст: электронный

16. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. Автоматизированная библиотечная информационная система Unilib UC : версия 2.110 // Научная библиотека Донецкого национального университета экономики и торговли им. Михаила Туган-Барановского. – [Донецк, 2021–]. – Текст: электронный.

2. Информио: электрон. справочник / ООО «РИНФИЦ». – Москва: Издат. дом «Информио», [2018?–]. – URL: https://www.informio.ru (дата обращения: 01.01.2023). – Текст:

электронный.

3. IPR SMART: весь контент ЭБС Ipr books: цифровой образоват. ресурс / ООО «Ай Пи Эр Медиа». – [Саратов: Ай Пи Эр Медиа, 2022]. – URL: http://www.iprbookshop.ru (дата обращения: 01.01.2023). – Режим доступа: для авториз. пользователей. – Текст. Аудио. Изображения: электронные.

4. Лань: электрон.-библ. система. – Санкт-Петербург: Лань, cop. 2011–2021. – URL: https://e.lanbook.com/ (дата обращения: 01.01.2023). – Текст: электронный. – Режим доступа: для авторизир. пользователей.

5. СЭБ: Консорциум сетевых электрон. б-к / Электрон.-библ. система «Лань» при поддержке Агентства стратег. инициатив. – Санкт-Петербург: Лань, cop. 2011–2021. – URL: https://seb.e.lanbook.com/ (дата обращения: 01.01.2023). – Режим доступа: для пользователей организаций – участников, подписчиков ЭБС «Лань».

6. Polpred: электрон. библ. система : деловые статьи и интернет-сервисы / ООО «Полпред Справочники». – Москва: Полпред Справочники, cop. 1997–2022. – URL: https://polpred.com (дата обращения: 01.01.2023). – Текст: электронный.

7. Book on lime: дистанц. образование / изд-во КДУ МГУ им. М.В. Ломоносова. – Москва: КДУ, cop. 2017. – URL: https://bookonlime.ru (дата обращения: 01.01.2023) – Текст. Изображение. Устная речь: электронные.

8. Научная электронная библиотека elibrary.ru: информ.-аналит. портал / ООО Научная электронная библиотека. – Москва: ООО Науч. электрон. б-ка, cop. 2000–2022. – URL: https://elibrary.ru (дата обращения: 01.01.2023). – Режим доступа: для зарегистрир. пользователей. – Текст: электронный.

9. cyberleninka: науч. электрон. б-ка «КиберЛенинка» / [Е. Кисляк, Д. Семячкин, М. Сергеев; ООО «Итеос»]. – Москва: КиберЛенинка, 2012–. – URL: http://cyberleninka.ru (дата обращения: 01.01.2023). – Текст: электронный.

10. Национальная электронная библиотека: НЭБ: федер. гос. информ. система / М-во культуры Рос. Федерации [и др.]. – Москва: Рос. гос. б-ка: ООО ЭЛАР, [2008–]. – URL: https://rusneb.ru/ (дата обращения: 01.01.2023) – Текст. Изображение: электронные.

11. Научно-информационный библиотечный центр имени академика Л.И. Абалкина / Рос. экон. ун-т им. В.Г. Плеханова. – Москва: KnowledgeTree Inc., 2008–. – URL: http://liber.rea.ru/login.php (дата обращения: 01.01.2023). – Режим доступа: для авторизир. пользователей. – Текст: электронный.

12. Библиотечно-информационный комплекс / Финансовый ун-т при Правительстве Рос. Федерации. – Москва: Финансовый университет, 2019–. – URL: http://library.fa.ru/ (дата обращения: 01.01.2023) – Режим доступа: для авторизир. пользователей. – Текст: электронный.

13. Университетская библиотека онлайн: электрон. библ. система. – ООО «Директ-Медиа», 2006–. – URL: https://biblioclub.ru/ (дата обращения: 01.01.2023) – Режим доступа: для авторизир. пользователей. – Текст: электронный.

14. Электронный каталог Научной библиотеки Донецкого национального университета экономики и торговли им. Михаила Туган-Барановского. – Донецк: НБ ДОННУЭТ, 1999–. – URL: http://catalog.donnuet.education (дата обращения: 01.01.2023). – Текст: электронный.

17. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Практические занятия проводятся в компьютерных классах, оборудованных современной компьютерной техникой с соответствующим программным обеспечением, возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Университета, устройствами для вывода на печать созданных документов, копировальной и сканирующей техникой.

Лекционные занятия проводятся в аудитории, оснащенной мультимедийной техникой для визуализации информации большой аудитории.

18. КАДРОВОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Фамилия, имя, отчество	Условия привлечения (по основному месту работы, на условиях внутреннего/ внешнего совместительства; на условиях договора гражданско-правового характера (далее – договор ГПХ)	Должность, ученая степень, ученое звание	Уровень образования, наименование специальности, направления подготовки, наименование присвоенной квалификации	Сведения о дополнительном профессиональном образовании
Пальчикова Наталья Сергеевна	по основному месту работы	Должность – старший преподаватель, ученая степень – нет, ученое звание - нет	Высшее, специальность «Экономика предприятия», квалификация экономист	1.Удостоверение о повышении квалификации ФГБОУ ВО «Донской государственный технический университет» программа повышения квалификации «Актуальные вопросы преподавания в образовательных учреждениях высшего образования: нормативно-правовое, психолого-педагогическое и методическое сопровождение» № 1-14500 от 24.09.2022 г. 2. Удостоверение о повышении квалификации ФГБОУ ВО «Донской государственный технический университет» программа повышения квалификации «Организационно-методические аспекты разработки и реализации программ высшего образования по направлениям подготовки Информационная безопасность» № 1-18066 от 09.06.2023 г. 3. Акционерное общество «Академия «Просвещение»» удостоверение о повышении квалификации по дополнительной профессиональной программе «Организация комплексной работы с высокотехнологичным лабораторным оборудованием» (№ ПК-АП-2023-ОКР-ВЛО-2045 от 29.11.2023 г.) 2. Безопасная молодежная среда. Программа Росмолодежь. Сертификат о повышении квалификации «Информационная безопасность» (№ОПРДМ-37474-А1817 от 24.05.2024)

Б 1.О.15 **ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

Специальность 38.05.02 Таможенное дело
Специализация Таможенные платежи и валютное регулирование

Трудоемкость учебной дисциплины: 4 з.е.

В результате изучения учебной дисциплины обучающийся должен:

знать: базовый понятийный аппарат в области информационной безопасности; принципы и общие методы обеспечения информационной безопасности; критерии, условия и принципы отнесения информации к защищаемой; принципы и методы обработки конфиденциальных документов; методы и приемы защиты документированной информации от несанкционированного доступа;

уметь: практически выполнять технологические операции по защите и обработке конфиденциальных документов; разрабатывать политику предприятия в соответствии со стандартами безопасности; применить и настроить различные средства защиты информации; оценивать качество информационных ресурсов.

владеть: методами и формами защиты информации; технологией составления конфиденциальных документов; практическими навыками применения средств защиты информации при решении профессиональных задач, приёмами социальной адаптации информационных ресурсов и информационных технологий.

В результате освоения учебной дисциплины обучающийся должен обладать такими компетенциями:

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.2 Разрабатывает варианты решения проблемной ситуации на основе критического анализа доступных источников информации

Наименование смысловых модулей и тем учебной дисциплины:

Смысловой модуль 1. Информационная безопасность в экономических информационных системах. Тема 1. Введение в информационную безопасность. Модели информационной безопасности. Тема 2. Выявление возможных нарушений и атак в экономических информационных системах (ЭИС).

Смысловой модуль 2. Инструменты защиты информации в экономических информационных системах. Тема 3. Противодействие вредоносным программам в ЭИС. Тема 4. Применение криптографических систем шифрования данных. Тема 5. Методы защиты информации в корпоративных вычислительных сетях (Интранет). Тема 6. Методы защиты информации в глобальной сети Интернет.

Смысловой модуль 3. Проверка состояния информационной безопасности в экономических информационных системах.Тема 7. Аудит информационной безопасности. Тема 8. Анализ информационных рисков.

Форма промежуточной аттестации: экзамен
(зачет с оценкой, экзамен)

Разработчик:
Пальчикова Н.С.

Заведующий кафедрой информационных систем
и технологий управления
Бессарабов В.О., д.э.н., профессор

КАФЕДРА ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ УПРАВЛЕНИЯ