МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тверской государственный технический университет»
(ТвГТУ)

УТВЕРЖДАЮ
Проректор по учебно-
воспитательной работе
_____ Э.Ю. Майкова
« _____ » _____ 2019 г.

РАБОЧАЯ ПРОГРАММА

дисциплина обязательной части Блока 1
«Информационная безопасность»

по специальности
38.05.01 Экономическая безопасность

Направленность (специализация)
Экономико-правовое обеспечение экономической безопасности

Типы задач профессиональной деятельности – информационно-аналитический, организационно-управленческий, научно-исследовательский

Форма обучения – очная, заочная

Факультет управления и социальных коммуникаций
Кафедра экономики и управления производством

Семестр 9

Тверь 2019

Рабочая программа дисциплины соответствует ОХОП подготовки специалистов в части требований к результатам обучения по дисциплине и учебному плану.

Разработчик программы: доцент кафедры ИС И.В. Мартынов

Программа рассмотрена и одобрена на заседании кафедры ЭУП
«11» ноября2019 г., протокол № 2.

Заведующий кафедрой ЭУП О.М. Дюжилова

Согласовано

Начальник учебно-методического
отдела УМУ Д.А. Барчуков

Начальник отдела
комплектования
зональной научной библиотеки О.Ф. Жмыхова

1. Цель и задачи дисциплины

Целью изучения дисциплины «Информационная безопасность» является ознакомление обучающихся с основными средствами, механизмами и методами их применения, направленными на обеспечение информационной безопасности и защите информации деятельности хозяйствующего субъекта.

Задачами дисциплины являются:

- сформировать общее представление об информационной безопасности как о состоянии защищенности информационного ресурса сложной системы, включая аппаратную часть и математическое обеспечение;
- сформировать навыки по обеспечению защиты объектов интеллектуальной собственности и результатов исследований и разработок как коммерческой тайны предприятия;
- сформировать навыки работы с методами криптографии и криптоанализа;
- сформировать у студентов системы знаний в области информационной безопасности и применения на практике методов и средств защиты информации.
- сформировать навыки практической реализации типовых мероприятий по обеспечению информационной безопасности и защите информации;
- сформировать навыки анализа информационных ресурсов по следующим факторам: важность, конфиденциальность, уязвимость.

2. Место дисциплины в структуре ОП.

Дисциплина относится к обязательной части Блока 1 ОП ВО, формируемых участниками образовательного процесса. Для освоения дисциплины «Информационная безопасность» студенты используют знания, умения и навыки, сформированные в ходе изучения дисциплин «Уголовное право и уголовный процесс», «Административное право», «Информатика», «Управление интеллектуальной собственностью», «Экономические преступления», «Теория систем и системный анализ», «Информационные системы в экономике», «Контроль и надзор деятельности хозяйствующих субъектов», «Экономическая безопасность хозяйствующих субъектов».

Дисциплина «Информационная безопасность» служит неотъемлемым дополнением дисциплин, профессиональная подготовка по которым предполагает использование приобретенных знаний при решении профессиональных задач и при выполнении выпускной квалификационной работы.

3. Планируемые результаты обучения по дисциплине

3.1. Перечень компетенций, закреплённых за дисциплиной в ОХОП

ОПК-7. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.

Индикаторы компетенции, закреплённые за дисциплиной в ОХОП:

ИОПК-7.2Использует технологии защиты информации, программное обеспечение и современные информационные системы по управлению рисками для обеспечения информационной безопасности

Показатели оценивания индикаторов достижения компетенций

Знать:

З1.1. Источники возникновения информационных угроз.
З1.2. Каналы утечки информации.
З1.3. Направления и средства защиты информации.
З1.4. Принципы национальной безопасности.
З1.5. Прогрессивные исследования, ведущиеся в области информационной безопасности.
З1.6. Методы и приемы анализа информации.
З1.7. Математические принципы, лежащие в основе криптографических моделей.
З1.8. Порядок проведения анализа информационной безопасности объектов и систем.

Уметь:

У1.1. Применять организационные, технические и программные средства защиты информации.
У1.2. Выявлять потенциальные каналы утечки информации и определять их характеристики.
У1.3. Выбирать, адаптировать и применять необходимые алгоритмы при решении профессиональных задач.
У1.4. Использовать алгоритмические модели и языки программирования для разработки алгоритмов шифрования.
У1.5. Разрабатывать и обосновывать варианты эффективных управленческих решений в области информационной безопасности.

3.2. Технологии, обеспечивающие формирование компетенций

Проведение лекционных и лабораторных занятий.

4. Трудоемкость дисциплины и виды учебной работы

ОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 1а. Распределение трудоемкости дисциплины по видам учебной работы

Вид учебной работы	**Зачетные единицы**	**Академические часы**
Общая трудоемкость дисциплины	3	108
Аудиторные занятия (всего)		42
В том числе:		
Лекции		21
Практические занятия (ПЗ)		не предусмотрены
Лабораторные работы (ЛР)		21
Самостоятельная работа обучающихся (всего)		66

В том числе:		
Курсовая работа		не предусмотрена
Курсовой проект		не предусмотрен
Расчетно-графические работы		не предусмотрены
Другие виды самостоятельной работы: - подготовка к лабораторным занятиям		60
Текущий контроль успеваемости и промежуточная аттестация (зачет)		6
Текущий контроль успеваемости и промежуточная аттестация (экзамен)		не предусмотрен
Практическая подготовка при реализации дисциплины (всего)		0

ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 1б. Распределение трудоемкости дисциплины по видам учебной работы

Вид учебной работы	**Зачетные единицы**	**Академические часы**
Общая трудоемкость дисциплины	3	**108**
Аудиторные занятия (всего)		**8**
В том числе:		
Лекции		4
Практические занятия (ПЗ)		не предусмотрены
Лабораторные работы (ЛР)		4
Самостоятельная работа обучающихся (всего)		**96+4(зачет)**
В том числе:		
Курсовая работа		не предусмотрена
Курсовой проект		не предусмотрен
Расчетно-графические работы		не предусмотрены
Другие виды самостоятельной работы: - подготовка к лабораторным занятиям		96
Текущий контроль успеваемости и промежуточная аттестация (зачет)		4
Текущий контроль успеваемости и промежуточная аттестация (экзамен)		не предусмотрен
Практическая подготовка при реализации дисциплины (всего)		0

5. Структура и содержание дисциплины

5.1. Структура дисциплины

ОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 2а. Модули дисциплины, трудоемкость в часах и виды учебной работы

№	Наименование модуля	Труд-ть часы	Лекции	Практич. занятия	Лаб. работы	Сам. работа
1 семестр						
1	Модуль 1. Основы понятия и практического значения информационной безопасности	42	7	-	7	28
2	Модуль 2. Методы и средства обеспечения информационной безопасности хозяйствующих субъектов	66	14	-	14	38
	Всего на дисциплину	**108**	**21**	**-**	**21**	**66**

ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ

№	Наименование модуля	Труд-ть часы	Лекции	Практич. занятия	Лаб. работы	Сам. работа
1 семестр						
1	Модуль 1. Основы понятия и практического значения информационной безопасности	35	1	-	1	32+1(зачет)
2	Модуль 2. Методы и средства обеспечения информационной безопасности хозяйствующих субъектов	73	3	-	3	64+3(зачет)
	Всего на дисциплину	**108**	**4**	**-**	**4**	**96+4(зачет)**

5.2. Содержание дисциплины

Модуль 1 «ОСНОВЫ ПОНЯТИЯ И ПРАКТИЧЕСКОГО ЗНАЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Тема 1. Информационная безопасность в системе национальной безопасности РФ

Профессиональная терминология при изучении курса. Актуальность проблемы недостаточного обеспечения информационной безопасности на всех уровнях мирового сообщества. Суть, методы и средства информационной войны. Основные составляющие информационной безопасности (конфиденциальность, целостность, доступность, объекты информационной безопасности, статистика нарушений информационной безопасности, описание наиболее характерных случаев и примеров, последствия).

Тема 2. Нормативно-правовые механизмы обеспечения информационной безопасности

Законодательный уровень информационной безопасности РФ и его важность (обзор российского законодательства в области информационной безопасности).

Обзор зарубежного законодательства в области информационной безопасности.

Модуль 2 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФРМАЦИОННОЙ БЕЗОПАСНОСТИ ХОЗЯЙСТВУЮЩИХ СУБЪЕКТОВ»

Тема 3. Основные определения и критерии классификации угроз.

Угрозы доступности, уничтожение информационных объектов, утечка информации, искажение информации, блокирование объекта информации с примерами и последствиями.

Вредоносное программное обеспечение, действия пользователей, внутренние и внешние угрозы. Стандарты и спецификации в области информационной безопасности.

Тема 4. Основные принципы и уровни информационной безопасности

Классификация принципов и уровней информационной безопасности. Особенности технического обеспечения информационной безопасности в зависимости от уровня ее обеспечения.

Анализ рисков в области защиты информации хозяйствующих субъектов и этапы управления ими.

Анализ актуального состояния в области обеспечения информационной безопасности на российских предприятиях (практические примеры их использования).

5.3. Практические занятия.

Учебным планом не предусмотрены.

5.5. Лабораторный практикум.

Общая цель проведения лабораторных занятий – закрепление теоретических знаний, полученных в ходе самостоятельного изучения дисциплины о значении и методах обеспечения информационной безопасности хозяйствующих субъектов, необходимые специалисту в профессиональной деятельности.

Таблица 3а. Лабораторные занятия и их трудоемкость

Порядковый номер модуля. Цели лабораторных занятий	**Наименование лабораторных занятий**	**Трудоем-кость в часах**
Модуль 1 **Цель:** формирование системного мышления о необходимости обеспечения информационной безопасности объектов от внутренних и внешних угроз, способных нанести ущерб на микро- и макроуровнях	1. Информационная безопасность в условиях функционирования в России глобальных сетей. 2. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. 3. Классификация видов нарушителей информационной безопасности. 4. Анализ отечественной и зарубежной законодательной базы , а также нормативных документов в области обеспечения государственной, коммерческой и личной тайны.	7
Модуль 2 **Цель:** формирование умения применять на практике теоретические знания по обеспечению информационной безопасности, необходимую для обеспечения экономической безопасности хозяйствующего субъекта	5. Виды возможных нарушений информационной системы. 6. Анализ способов нарушений информационной безопасности. 7. Способы защиты от возможных нарушений безопасности информационной системы. 8. Методы криптографии и основные технологии построения защищенных систем. 9.Основныемеханизмы предотвращения угроз и способы управления рисками информационной безопасности	14

ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ

Порядковый номер модуля. Цели лабораторных занятий	**Наименование лабораторных занятий**	**Трудоем-кость в часах**
Модуль 1 **Цель:** формирование системного мышления о необходимости обеспечения информационной безопасности объектов от внутренних и внешних угроз, способных нанести ущерб на микро- и макроуровнях	1. Информационная безопасность в условиях функционирования в России глобальных сетей. 2. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. 3. Классификация видов нарушителей информационной безопасности. 4. Анализ отечественной и зарубежной законодательной базы , а также нормативных документов в области обеспечения государственной, коммерческой и личной тайны.	1
Модуль 2 **Цель:** формирование умения применять на практике теоретические знания по обеспечению информационной безопасности, необходимую для обеспечения экономической безопасности хозяйствующего субъекта	5. Виды возможных нарушений информационной системы. 6. Анализ способов нарушений информационной безопасности. 7. Способы защиты от возможных нарушений безопасности информационной системы. 8. Методы криптографии и основные технологии построения защищенных систем. 9.Основныемеханизмы предотвращения угроз и способы управления рисками информационной безопасности	3

6.Самостоятельная работа обучающихся и текущий контроль успеваемости.

6.1. Цели самостоятельной работы

Формирование способностей к самостоятельному познанию и обучению, поиску необходимой литературы, обобщению, проработке и закреплению теоретических знаний в рамках изучаемой дисциплины для формирования умений их практического применения в соответствии с гражданской позицией и нормами действующего законодательства в своей профессиональной деятельности.

6.2. Организация и содержание самостоятельной работы

Самостоятельная работа заключается в изучении отдельных тем курса по заданию преподавателя по рекомендуемой им учебной литературе, в подготовке к

лабораторным работам и их защитам, к текущему контролю успеваемости и промежуточной аттестации – «зачет».

Тематика самостоятельной работы имеет профессионально-ориентированный характер и непосредственную связь рассматриваемых вопросов с будущей профессиональной деятельностью выпускника, т.е. иметь системно-деятельностную направленность.

В рамках дисциплины проводятся лабораторные работы, защита которых производится непосредственно на занятии при выполнении определенного комплекса физических нагрузок. Максимальная оценка за каждую выполненную лабораторную работу – 5 баллов, минимальная – 3 балла.

Выполнение лабораторных работ обязательно. В случае не явки на лабораторное занятие по уважительной причине студент имеет возможность выполнить письменный реферат, по согласованной с преподавателем теме по модулю, по которому пропущено лабораторное занятие. Возможная тематическая направленность реферативной работы для каждого учебно-образовательного модуля представлена в следующей таблице 4.

Таблица 4. Темы рефератов

№ п/п	Модули	Возможная тематика самостоятельной реферативной работы
1.	**Модуль 1**	1. Угрозы информационной безопасности предприятия (организации) и способы борьбы с ними. 2. Сущность понятия «Национальная безопасность». 3.Анализ законодательства РФ в области информационной безопасности. 4. Анализ зарубежных стран в области информационной безопасности. 5. Сущность информационной войны. 6. Оценка ущерба от нарушения защиты информационной безопасности хозяйствующего субъекта. 7. Оценка ущерба от нарушения информационной безопасности государственных учреждений.
2.	**Модуль 2**	8. Главная задача специалиста по обеспечению информационной безопасности. 9. Современные средства защиты информации. 10.Современные системы компьютерной безопасности. 11. Современные средства противодействия экономическому шпионажу. 12. Современные криптографические системы. 13.Криптоанализ, современное состояние. 14. Современные требования, меры и рекомендации по обеспечению технической защиты информации и обеспечения информационной безопасности. 15. Современные методы защиты от атак на систему безопасности. 16. Современные методы управления рисками информационной безопасности.

Оценивание в этом случае осуществляется путем устного опроса по содержанию и качеству выполненной реферативной работы.

При отрицательных результатах по формам текущего контроля и (или) наличии пропусков преподаватель проводит с обучающимся индивидуальную работу по ликвидации задолженности.

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Основная литература

1. Милешко, Л.П. Экономика и менеджмент безопасности : учебное пособие для вузов / Л.П. Милешко. - Москва : Юрайт, 2022. - (Высшее образование). - Образовательная платформа Юрайт. - Текст : электронный. - Режим доступа: по подписке. - Дата обращения: 07.07.2022. - ISBN 978-5-534-13764-4. - URL: https://urait.ru/bcode/496722 . - (ID=139267-0)

2. Корабельников, С.М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С.М. Корабельников. - Москва : Юрайт, 2022. - (Высшее образование). - Образовательная платформа Юрайт. - Текст : электронный. - Режим доступа: по подписке. - Дата обращения: 07.07.2022. - ISBN 978-5-534-12769-0. - URL: https://urait.ru/book/prestupleniya-v-sfere-informacionnoy-bezopasnosti-496492 . - (ID=135845-0)

3. Нестеров, С.А. Основы информационной безопасности : учебное пособие / С.А. Нестеров. - 5-е изд. ; стер. - Санкт-Петербург [и др.] : Лань, 2022. - (Учебники для вузов. Специальная литература). - ЭБС Лань. - Текст : электронный. - Режим доступа: по подписке. - Дата обращения: 25.08.2022. - ISBN 978-5-8114-4067-2. - URL: https://e.lanbook.com/book/206279 . - (ID=113816-0)

7.2. Дополнительная литература

1. Гостев, И.М. Операционные системы : учебник и практикум для вузов : в составе учебно-методического комплекса / И.М. Гостев. - 2-е изд. ; испр. и доп. - Москва : Юрайт, 2022. - (Высшее образование) (УМК-У). - Образовательная платформа Юрайт. - Текст : электронный. - Режим доступа: по подписке. - Дата обращения: 07.07.2022. - ISBN 978-5-534-04520-8. - URL: https://urait.ru/bcode/490157 . - (ID=145044-0)

2. Информационное право : учебник для вузов / М.А. Федотов [и др.]; под редакцией М.А. Федотова. - Москва : Юрайт, 2022. - (Высшее образование). - Образовательная платформа Юрайт. - Текст : электронный. - Режим доступа: по подписке. - Дата обращения: 07.07.2022. - ISBN 978-5-534-10593-3. - URL: https://urait.ru/book/informacionnoe-pravo-489946 . - (ID=140486-0)

3. Суворова, Г.М. Информационная безопасность : учебное пособие для вузов / Г.М. Суворова. - Москва : Юрайт, 2022. - (Высшее образование). - Образовательная платформа Юрайт. - Текст : электронный. - Режим доступа: по подписке. - Дата обращения: 07.07.2022. - ISBN 978-5-534-13960-0. - URL: https://urait.ru/bcode/496741 . - (ID=139087-0)

7.3. Методические материалы

1. Учебно-методический комплекс элективной дисциплины части, формируемой участниками образовательных отношений Блока 1 "Информационная безопасность" направления подготовки 38.05.01 Экономическая безопасность. Направленность (специализация): Экономико-правовое обеспечение экономической безопасности : ФГОС 3++ / Каф. Экономика и управление производством ; разраб.: И.В. Мартынов. - 2022. - (УМК). - Текст : электронный. - 0-00. - URL: https://elib.tstu.tver.ru/MegaPro/GetDoc/Megapro/116212 . - (ID=116212-1)

7.4. Программное обеспечение по дисциплине

1. Операционная система Microsoft Windows: лицензии № ICM-176609 и № ICM-176613 (Azure Dev Tools for Teaching).

2. Microsoft Office 2019 Russian Academic: OPEN No Level: лицензия № 41902814.

7.5. Специализированные базы данных, справочные системы, электронно-библиотечные системы, профессиональные порталы в Интернет.

ЭБС и лицензионные ресурсы ТвГТУ размещены:

1. Ресурсы:https://lib.tstu.tver.ru/header/obr-res
2. ЭКТвГТУ:https://elib.tstu.tver.ru/MegaPro/Web
3. ЭБС "Лань":https://e.lanbook.com/
4. ЭБС "Университетская библиотека онлайн":https://www.biblioclub.ru/
5. ЭБС «IPRBooks»:https://www.iprbookshop.ru/
6. Электронная образовательная платформа "Юрайт" (ЭБС «Юрайт»):https://urait.ru/
7. Научная электронная библиотека eLIBRARY:https://elibrary.ru/
8. Информационная система "ТЕХНОРМАТИВ". Конфигурация "МАКСИМУМ" : сетевая версия (годовое обновление): [нормативно-технические, нормативно-правовые и руководящие документы (ГОСТы, РД, СНиПы и др.]. Диск 1,2,3,4. - М. :Технорматив, 2014. - (Документация для профессионалов). - CD. - Текст : электронный. - 119600 р. – (105501-1)
9. База данных учебно-методических комплексов:https://lib.tstu.tver.ru/header/umk.html

УМК размещен: https://elib.tstu.tver.ru/MegaPro/GetDoc/Megapro/116212

8. Материально-техническое обеспечение

При изучении дисциплины «Информационная безопасность» используются современные средства обучения: наглядные пособия, схемы карт-процессов, занятия проводятся в компьютерном классе, компьютеры которого объединены в локальную сеть. Возможна демонстрация учебного материала с помощью проектора.

9. Фонд оценочных средств промежуточной аттестации

9.1. Фонд оценочных средств промежуточной аттестации в форме экзамена

Учебным планом экзамен по дисциплине не предусмотрен.

9.2. Фонд оценочных средств для проведения промежуточной аттестации в форме зачёта

1. Вид промежуточной аттестации в форме зачета.

Вид промежуточной аттестации устанавливается преподавателем:

по результатам текущего контроля знаний и умений обучающегося без дополнительных контрольных испытаний;

по результатам выполнения дополнительного итогового контрольного испытания при наличии у студентов задолженностей по текущему контролю.

2. При промежуточной аттестации без выполнения дополнительного итогового контрольного испытания студенту в обязательном порядке описываются критерии проставления зачёта:

«зачтено» - выставляется обучающемуся при условии выполнения им всех контрольных мероприятий: посещение лекций в объеме не менее 80% контактной работы с преподавателем, выполнения и защиты лабораторных работ.

При промежуточной аттестации с выполнением заданий дополнительного итогового контрольного испытания студенту выдается билет с вопросами и задачами.

Число заданий для дополнительного итогового контрольного испытания - 15.

Число вопросов – 3 (2 вопроса для категории «знать» и 1 вопрос для категории «уметь»).

Продолжительность – 60 минут.

3. Шкала оценивания промежуточной аттестации – «зачтено», «не зачтено».

4. Критерии выполнения контрольного испытания и условия проставления зачёта:

для категории «знать» (бинарный критерий):

ниже базового - 0 балл;

базовый уровень – 1 балла;

критерии оценки и ее значение для категории «уметь» (бинарный критерий):

отсутствие умения – 0 балл;

наличие умения – 1 балла.

Критерии итоговой оценки за зачет:

«зачтено» - при сумме баллов 2 или 3;

«не зачтено» - при сумме баллов 0 или 1.

5. Для дополнительного итогового контрольного испытания студенту в обязательном порядке предоставляется:

база заданий, предназначенных для предъявления обучающемуся на дополнительном итоговом контрольном испытании (типовой образец задания приведен в Приложении);

методические материалы, определяющие процедуру проведения дополнительного итогового испытания и проставления зачёта.

6. Задание выполняется письменно.

Перечень вопросов дополнительного итогового контрольного испытания:

1. Понятие информационной безопасности и особенности ее обеспечения.

2. Основные составляющие информационной безопасности.
3. Основы государственной политики обеспечения информационной безопасности Российской Федерации и правовые акты и законы.
4. Законодательный уровень информационной безопасности, важность.
5. Роль и место информационной войны в мире.
6. Средства ведения электронных информационных войн.
7. Вопросы защиты информации как составляющая общей проблемы обеспечения информационной безопасности.
8. Обзор зарубежного законодательства в области информационной безопасности.
9. Основные принципы обеспечения информационной безопасности.
10. Основные уровни информационной безопасности.
11. Обобщенная модель угроз. Внешние и внутренние угрозы.
12. Классификация угроз.
13. Стандарты обеспечения информационной безопасности.
14. Спецификации информационной безопасности.
15. Механизмы информационной безопасности.
16. Классы информационной безопасности.
17. Характеристики возможных угроз. Объекты возможных угроз. Виды возможных угроз.
18. Меры и средства защиты от угроз.
19. Меры противодействия внешним угрозам.
20. Меры противодействия внутренним угрозам.
21. Общие требования к комплексу защиты информации.
22. Общие требования к программно-техническим средствам защиты информации.
23. Угрозы информации: угрозы секретности, угрозы целостности.
24. Управление рисками информационной безопасности.
25. Политика безопасности.
26. Классификация систем защиты.
27. Роль стандартов информационной безопасности.
28. Административный уровень информационной безопасности.
29. Процедурный уровень информационной безопасности
30. Аппаратно-программные средства защиты информации, классификация и их применение.
31. Основные этапы реализации информационной безопасности.
32. Информационная безопасность распределенных систем.
33. Сетевые сервисы и механизмы безопасности, администрирование средств безопасности.

Пользование различными техническими устройствами, кроме ЭВМ компьютерного класса и программным обеспечением, необходимым для решения поставленных задач, не допускается. При желании студента покинуть пределы аудитории во время экзамена экзаменационный билет после его возвращения заменяется.

Преподаватель имеет право после проверки письменных ответов вопросы задавать студенту в устной форме уточняющие вопросы в рамках задания, выданного студенту.

9.3. Фонд оценочных средств промежуточной аттестации в форме курсового проекта или курсовой работы

Учебным планом не предусмотрена промежуточная аттестация в форме курсовой работы.

10. Методические рекомендации по организации изучения дисциплины.

Студенты перед началом изучения дисциплины ознакомлены с системами кредитных единиц и балльно-рейтинговой оценки.

Студенты, изучающие дисциплину, обеспечиваются электронными изданиями или доступом к ним, учебно-методическим комплексом по дисциплине, включая методические указания к выполнению практических, контрольных работ, всех видов самостоятельной работы.

В учебный процесс рекомендуется внедрение субъект-субъектной педагогической технологии, при которой в расписании каждого преподавателя определяется время консультаций студентов по закрепленному за ним модулю дисциплины.

11. Внесение изменений и дополнений в рабочую программу дисциплины

Кафедра ежегодно обновляет содержание рабочих программ дисциплин, которые оформляются протоколами заседаний дисциплин, форма которых утверждена Положением о рабочих программ дисциплин, соответствующих ФГОС ВО.

Приложение

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тверской государственный технический университет»

Специальность 38.05.01 Экономическая безопасность
Направленность (специализация) – Экономико-правовое обеспечение экономической безопасности
Кафедра «Экономика и управление производством»
Дисциплина «Информационная безопасность»
Семестр 9

ЗАДАНИЕ ДЛЯ ДОПОЛНИТЕЛЬНОГО ИТОГОВОГО КОНТРОЛЬНОГО ИСПЫТАНИЯ №_1_

1. Задание для проверки уровня «знать» – или 0, или 1 балл:
Информационная война: понятие и сущность.

2. Задание для проверки уровня «знать» – или 0, или 1 балл:
Характеристики возможных угроз при осуществлении предпринимательской деятельности.

3. Задание для проверки уровня «уметь» – или 0, или 1 балл:
Описать базовые методы парольной аутентификации.

Критерии итоговой оценки:
«зачтено» - при сумме баллов 2 или 3;
«не зачтено» - при сумме баллов 0 или 1;

Составитель: доцент кафедры ИС _____ И.В. Мартынов

Заведующий кафедрой ЭУП, д.э.н., _____О.М. Дюжилова