МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
высшего образования - программы бакалавриата
по направлению подготовки
41.03.05 Международные отношения,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Информационная безопасность на объектах транспортной инфраструктуры

Направление подготовки: 41.03.05 Международные отношения

Направленность (профиль): Мировая политика и международное (транспортное) право

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Учебная дисциплина (модуль) «Информационная безопасность на объектах транспортной инфраструктуры» относится к блоку 1 "Дисциплины (модули)" и входит в вариативную часть по направлению подготовки/специальности 41.03.05 – Международные отношения и профилю подготовки Мировая политика и международное транспортное право.

Целью дисциплины "Информационная безопасность на объектах транспортной инфраструктуры" является усвоение студентами основ информационной безопасности, этапов ее развития, состояние информационной безопасности на современном этапе

Задачи обучения дисциплине «Информационная безопасность на объектах транспортной инфраструктуры»:

- обеспечение усвоения студентами основных концептов и категорий основ информационной безопасности и умения оперировать ими;
- формирование умения самостоятельно анализировать угрозы и вызовы информационной безопасности;
- ознакомление студентов с основными принципами построения и особенностями стратегий национальной и международной безопасности;
- обучение навыкам анализа концепций обеспечения национальной безопасности ведущих зарубежных стран;

2. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

ПК-1 - Способен осуществлять деловую переписку по вопросам заключения внешнеторгового контракта, в том числе с использованием современных информационных технологий и программных средств (текстовые, графические, табличные и аналитические приложения, приложения для визуального представления данных);

ПК-6 - Способен определять, находить и разрабатывать актуальные интересные темы для целевой аудитории;

ПК-7 - Способен анализировать большой объем информации.

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

Знать:

• Знание требований к защите информации определенного типа;

• средства и методы предотвращения и обнаружения вторжений;

• нормативно-правовые документы по обеспечению информационной безопасности

• организацию защиты, конфиденциальности и информационного сопровождения внешнеторгового контракта.

Уметь:

• оценивать качество готового программного обеспечения;

• работать с компьютером как средством управления информацией;

• анализировать большой объем информации;

• находить и разрабатывать актуальные интересные темы для целевой аудитории;

• пользоваться нормативными документами по информационной безопасности.

Владеть:

• сбора и обработки информации, имеющей значение для углубленного изучения проблем обеспечения информационной безопасности;

• основными способами обнаружения информационных угроз и использования современных антивирусных программ;

• поиска взаимоприемлемых компромиссных решений в ходе деловых переговоров, а также ведения деловой переписки и информационного сопровождения, по вопросам внешнеторгового контракта.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 2 з.е. (72 академических часа(ов).

3.2. Объем дисциплины (модуля) в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Тип учебных занятий	Количество часов	
	Всего	Сем. №8
Контактная работа при проведении учебных занятий (всего):	40	40
В том числе:		

Занятия лекционного типа	24	24
Занятия семинарского типа	16	16

3.3. Объем дисциплины (модуля) в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации составляет 32 академических часа (ов).

3.4. При обучении по индивидуальному учебному плану, в том числе при ускоренном обучении, объем дисциплины (модуля) может быть реализован полностью в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации.

4. Содержание дисциплины (модуля).

4.1. Занятия лекционного типа.

№ п/п	Тематика лекционных занятий / краткое содержание
1	Теоретические основы информационной безопасности. /Методологические основы и понятийный аппарат общей теории безопасности. Место общей теории безопасности в системе научных знаний. Основные понятия общей теории безопасности. Закон Российской Федерации «О безопасности» 1992 г. Личность. Общество. Государство. Жизненно важные интересы. Источники опасности. Вызов. Риск. Угроза. Опасность.
2	Роль информации в развитии общества. /Информационные революции, Информационное общество, Проблема информационного неравенства. Россия в информационной эпохе.
3	Анализ способов нарушений информационной безопасности./ Анализ различных способов нарушений информационной безопасности, Хакерские атаки, отказы оборудования в обслуживании, внешние факторы, влияющие прямо на информационную безопасность систем.
4	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. Организационные формы обеспечения безопасности в некрупных фирмах и малом бизнесе. Методы и средства защиты от вредоносных программ. Профилактика вирусного заражения программ. Защита информации в Интернете.
5	

№ п/п	Тематика лекционных занятий / краткое содержание
	Понятие информационных угроз и их виды. /Информационные угрозы. Угрозы нарушения конфиденциальности информации. Информационная атака. Потенциальные злоумышленники (хакеры, крекеры). 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. Исторические аспекты реализации информационных угроз. Способы воздействия угроз на информационные объекты. Компьютерные преступления и наказания: исторические примеры и современность. Риски угроз информационным ресурсам.
6	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. 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. Стандарты информационной безопасности.
7	Доктрина информационной безопасности Российской Федерации / национальные интересы Российской Федерации в информационной сфере, угрозы информационной безопасности Российской Федерации, правовые, организационные, технические средства обеспечения информационной безопасности, основные информационные угрозы и состояние информационной безопасности, негативные факторы, влияющие на состояние информационной безопасности, Информационная безопасность в области обороны страны, Состояние информационной безопасности в экономической сфере, стратегическая цель обеспечения информационной безопасности
8	Международные стандарты информационного обмена. /Информационная безопасность в условиях функционирования в России глобальных сетей, Стандарты в области информационной безопасности. Международные стандарты информационного обмена, Глобальные сети и информационная безопасность.
9	Конфиденциальная информация и её защита. /Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы./ Понятие государственной, коммерческой, личной тайны, Основные нормативные документы в этой области. Рассекречивание документов. Уровень тайны. Разглашение и утечка конфиденциальной информации (КИ).
10	Защита интеллектуальной собственности. / Международное право в сфере защиты информации. Защита авторских и смежных прав в законодательстве РФ. Объекты авторского права. Субъекты авторского права. Права обладателей авторских прав.
11	Место информационной безопасности экономических систем в национальной безопасности страны. /Информационная безопасность страны. Защита экономических систем, Обмен конфиденциальной информацией, Структура банковских информационных систем в области защиты информации, Важность защиты экономических систем, Электронные деньги и безопасность финансовых переводов, Концепция информационной безопасности
12	Влияние средств массовой информации. /Методы влияния СМИ на человеческое сознание, влияние просмотра сцен насилия по телевидению на поведение человека,

№ п/п	Тематика лекционных занятий / краткое содержание
	Дезинформация и конструирование информационной реальности, Информационный (общественный) резонанс, Общественное мнение, Стереотипы
13	Инновационное развитие современных транспортных систем и проблемы информационного терроризма. / Терроризм высоких технологий в системе транспортных коммуникаций: методология анализа и прогнозирования. Информационные технологии и личная безопасность.
14	Укрепление международной информационной безопасности (МИБ) как мегатренд современной мировой политики. /Резолюция ГА ООН (A/RES/68/243) «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», МИБ – особенности подхода США и их союзников, Двусторонний формат сотрудничества Россия-США в области МИБ, Нормативно-правовое обеспечение МИБ в России, Концепции внешней политики России о МИБ, Базовые положения «Основ государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года», Основные угрозы в области МИБ
15	Международно-правовые основы по обеспечению информационной безопасности./ Транснациональные сообщества. Системы коллективной безопасности. Международные договоры, доктрины в области ИБ. Международно-правовые основы деятельности государств по обеспечению информационной безопасности.
16	Информационная война: актуальные вызовы. / Кибертерроризм. Информационный терроризм, информационная война, Информационное оружие, Информационная атака, Стратегическое информационное противоборство

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Теоретические основы информационной безопасности. Групповая дискуссия: «Методологические основы и понятийный аппарат общей теории безопасности».
2	Роль информации в развитии общества. Групповая дискуссия: «Проблема информационного неравенства».
3	Анализ способов нарушений информационной безопасности. Групповая дискуссия: «Хакерские атаки как вызовы информационной безопасности».
4	Методы и средства обеспечения безопасности. Групповая дискуссия: «Защита информации в Интернете»
5	Понятие информационных угроз и их виды. Групповая дискуссия: «Классификация угроз безопасности информации»
6	Государственное регулирование информационной безопасности. Групповая дискуссия: «Исторические аспекты борьбы органов уголовной юстиции с компьютерной преступностью (опыт США, стран Западной Европы, России).»
7	Доктрина информационной безопасности Российской Федерации. Групповая дискуссия: «Угрозы информационной безопасности Российской Федерации»
8	Международные стандарты информационного обмена. Групповая дискуссия: «Информационная безопасность в условиях функционирования в России глобальных

№ п/п	Тематика практических занятий/краткое содержание
	сетей»
9	Конфиденциальная информация и её защита. Групповая дискуссия: «Понятие государственной, коммерческой, личной тайны: уровни доступа»
10	Защита интеллектуальной собственности. Групповая дискуссия: «Объекты авторского права»
11	Место информационной безопасности экономических систем в национальной безопасности страны. Групповая дискуссия: «Электронные деньги и безопасность»
12	Влияние средств массовой информации. Групповая дискуссия: «Дезинформация и конструирование информационной реальности СМИ»
13	Инновационное развитие современных транспортных систем и проблемы информационного терроризма. Групповая дискуссия: «Терроризм высоких технологий в системе транспортных коммуникаций»
14	Укрепление международной информационной безопасности (МИБ) как мегатренд современной мировой политики. Групповая дискуссия: «Основные угрозы в области МИБ»
15	Международно-правовые основы по обеспечению информационной безопасности. Групповая дискуссия: «Международно-правовые основы деятельности государств по обеспечению информационной безопасности»
16	Информационная война: актуальные вызовы. Групповая дискуссия: «Информационный терроризм»

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Подготовка к пратическому занятию "Теоретические основы информационной безопасности": -работа с лекционными материалами по теме; -чтение рекомендуемой литературы; -подготовка презентаций к занятию.
2	Подготовка к пратическому занятию "Роль информации в развитии общества": -работа с лекционными материалами по теме; -чтение рекомендуемой литературы; -подготовка презентаций к занятию.
3	Подготовка к пратическому занятию "Конфиденциальная информация и её защита": -работа с лекционными материалами по теме; -чтение рекомендуемой литературы; -подготовка презентаций к занятию.
4	Подготовка к пратическому занятию "Доктрита информационной безопасности Российской Федерации": -работа с лекционными материалами по теме; -чтение рекомендуемой литературы; -подготовка презентаций к занятию.
5	Подготовка к пратическому занятию "Укрепление международной информационной безопасности (МИБ) как мегатренд современной мировой политики": -работа с лекционными материалами по теме; -чтение рекомендуемой литературы; -подготовка презентаций к занятию.
6	Подготовка к промежуточной аттестации.
7	Подготовка к текущему контролю.

5. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

№ п/п	Библиографическое описание	Место доступа
1	Информационная безопасность : учебное пособие для вузов Г. М. Суворова Москва : Издательство Юрайт , 2021	НТБ РУТ (МИИТ) www.library.miit.ru
2	Информационная безопасность : учебник и практикум для академического бакалавриата С. А. Нестеров М. : Издательство Юрайт , 2017	НТБ РУТ (МИИТ) www.library.miit.ru
3	Информационная безопасность : учеб. пособие В.В. Гафнер Ростов н/Д : Феникс , 2010	http://xn--90akw.xn--p1ai/data/documents/IB-Gafner.pdf
4	Глобальная безопасность в цифровую эпоху: стратагемы для России Смирнова А.И М. : ВНИИгеосистем , 2014	https://mgimo.ru/upload/iblock/2d5/2d5686c9163ee863339211b841c8bf72.pdf

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении дисциплины (модуля).

Базы данных, информационно-справочные и поисковые системы:

НТБ РУТ (МИИТ) – http://library.miit.ru

www.e-library.ru,

Oxford Journals, Annual Reviews,

HighWire PRESS, IOP – Institute of Physics (Великобритания),

PNAS Online – Proceedings of National Academy of Sciences (США),

ProQuest Digital Dissertations,

Журналы издательства Sage, SCIENCE» - FREE,

Поисковая система «Science Research»,

База диссертаций Канады (Национальная библиотека Канады), База патентов США (United States Patent and Trademark Office)

Московский Центр Карнеги www.carnegie.ru (Журнал ProetContra)

Журнал «Политические исследования» (Полис) www.politstudies.ru.

Журнал «Полития» www.politeia.ru

Журнал «Социологические исследования» (Социс) www.isras.ru/socis.html

Журнал «Социально-гуманитарное знание» http://socgum-zhurnal.ru

Журнал «Вестник Московского университета», Серия 12 «Политические науки» http://polit.msu.ru/vestnik

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

1. Электронная информационно-образовательная среда РУТ (МИИТ), доступная из личного кабинета обучающегося или преподавателя на сайте http://miit.ru

2. Лицензионная операционная система MS Windows (академическая лицензия)

3. Лицензионный пакет программ Microsoft Office (академическая лицензия)

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

1. Учебные аудитории для проведения занятий, оснащенные проекционным и аудио оборудованием

2. Учебные аудитории для проведения групповых и индивидуальных консультаций

3. Учебные аудитории для проведения текущего контроля и промежуточной аттестации

4. Помещение для самостоятельной работы, оснащенное компьютерной техникой, подключенной к сети «Интернет» и доступом к электронно-

информационной образовательной среде университета

9. Форма промежуточной аттестации:

Зачет в 8 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы:

В.Н. Чигарев

Согласовано:

Заведующий кафедрой МОиГТ	В.Г. Егоров
Председатель учебно-методической комиссии	Г.А. Моргунова