

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
10.03.01 Информационная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Гуманитарные аспекты информационной безопасности

Направление подготовки: 10.03.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем

Форма обучения: Очная

Рабочая программа дисциплины (модуля) в виде
электронного документа выгружена из единой
корпоративной информационной системы управления
университетом и соответствует оригиналу

Простая электронная подпись, выданная РУТ (МИИТ)
ID подписи: 4196
Подписал: заведующий кафедрой Желенков Борис
Владимирович
Дата: 16.01.2023

1. Общие сведения о дисциплине (модуле).

Целью освоения дисциплины является формирование системного социально-ориентированного мышления студентов и умений: анализировать гуманитарные аспекты информационной безопасности, связанные с социальной сущностью информационных процессов в цифровом обществе; уметь критически оценивать и понимать процессы информационного воздействия на установки и поведение людей, как в ходе глобально ведущейся информационно-психологической борьбы за мировое влияние, так и в ходе получения информации ограниченного доступа потенциальными нарушителями при использовании так называемой «социальной инженерии»; уметь работать с персоналом организации по формированию навыков обеспечения информационной безопасности.

Задачи преподавания дисциплины:

- помочь студентам уяснить особенности гуманитарной составляющей информационной безопасности в её философских, политических, социально-психологических и других аспектах, атакуемых в информационно-психологическом противоборстве между государствами, а также потенциальными нарушителями информационной безопасности организации;
- оказать содействие процессам вузовского образовательно-воспитательного воздействия на сознание и чувства студентов для формирования у них активной гражданской позиции и умения отстаивать эту позицию в практической деятельности;
- сформировать практические навыки анализа и оценки содержания защищаемой информации и потенциальных угроз информационной безопасности личности, общества и государства, связанных с человеческим фактором;
- сформировать практические навыки работы с персоналом организации по обучению приемам обеспечения информационной безопасности, противостоянию потенциальным нарушителям с целью завладения информацией ограниченного доступа

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-13 - Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма;

ПК-4 - способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты ;

ПК-13 - способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности.

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

Знать:

- методологические основы гуманитарной составляющей информационной безопасности личности, общества и государства;
- основные теории информационно-психологических воздействий в политике и международных отношениях, в масштабах защищаемой организации и человека (как части информационной системы);
- сущность понятия «человеческий фактор» в системе информационной безопасности защищаемого объекта.

Уметь:

- выделять гуманитарные аспекты при формировании концепции информационной безопасности защищаемого объекта;
- понимать сущность, выделять и анализировать виды, средства, субъекты и мишени информационно-психологического воздействия при совершении информационных атак; планировать и организовывать работу по обеспечению информационной безопасности с учетом уязвимости «человеческого фактора».

Владеть:

- навыками выявления и противостояния приемам информационно-психологического воздействия противника в информационном противоборстве;
- применять навыки диагностики и противодействия манипулятивным методам, прогнозировать угрозы и вырабатывать методы и средства защиты от «социальной инженерии»;
- владеть эффективными методами и приемами обучения персонала вопросам информационной безопасности организации.

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):	52	52
В том числе:		
Занятия лекционного типа	26	26
Занятия семинарского типа	26	26

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 20 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	1. Введению в дисциплину «Гуманитарные аспекты информационной безопасности». Рассматриваемые вопросы: Методологические основы, цели и задачи дисциплины, связь с другими науками. Основное противоречие информационной безопасности личности. Роль информации в жизни человека. Человеческий фактор и его роль в обеспечении информационной безопасности. Риски цифровизации общества, «гуманизация» цифровизации.

№ п/п	Тематика лекционных занятий / краткое содержание
	<p>2. Теоретические аспекты развития информационного общества.</p> <p>Рассматриваемые вопросы: Информационные революции и развитие информационного общества. Основные теории информации. Информационные революции. Эволюция создания информационного общества, цифровой экономики и цифровизации общественных процессов. Социальные сети, их роль в развитии цифрового общества.</p> <p>3. Информационно-психологическое воздействие в международных отношениях и в масштабах защищаемой организации.</p> <p>Рассматриваемые вопросы: Психология воздействия и манипулирования. Принципы психологического воздействия. Понятие, виды, средства, субъекты и мишени информационно-психологического воздействия.</p> <p>4. Приемы психологического воздействия на личность и общество, способы защиты от манипулирования.</p> <p>Рассматриваемые вопросы: Психологическое воздействие и манипуляции: сходство и различие. Виды манипулирования. Побуждение и принуждение: скрытое и тайное. Манипулирование информацией. Манипулятивное воздействие. Манипулятивные технологии. Дезинформирование. Пропаганда. Способы защиты от манипуляций.</p> <p>5. Информационная война и методы её ведения. Средства ведения информационных войн.</p> <p>Рассматриваемые вопросы: Понятие информационных войн, сущность и методы ведения в работах отечественных и зарубежных ученых. Моральная, ментальная, физическая война. Кибервойна: кибератака, кибероборона, киберразведка. Информационное оружие, его характеристики. Средства информационно-психологического оружия: печатные материалы; средства массовой информации; интернет-ресурсы; когнитивное оружие.</p> <p>6. Информационные операции: понятие, виды, структура. Приемы информационного противоборства.</p> <p>Рассматриваемые вопросы: Информационная операция: структура, мишени, этапы. Информационный вброс. Алгоритм построения. Распознавание информационного вброса и меры противодействия и разоблачения. Пропаганда и контрпропаганда: понятие, виды, цели и мишени воздействия.</p> <p>7. Человеческий фактор в вопросах обеспечения информационной безопасности.</p> <p>Рассматриваемые вопросы: Понятие «человеческий фактор», учет его роли в обеспечении информационной безопасности организации. Социально-психологическая характеристика внутреннего и внешнего нарушителя, использование методов «социальной инженерии» для получения информации ограниченного доступа. Приемы противоборства методом «социальной инженерии».</p> <p>8. Вопросы ИБ в управлении персоналом.</p> <p>Рассматриваемые вопросы: Подбор персонала на должности, связанные с работой с информацией ограниченного доступа. Приемы обучения сотрудников навыкам обеспечения информационной безопасности в организации.</p>

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	<p>1. Введению в дисциплину «Гуманитарные аспекты информационной безопасности». В результате выполнения практического задания студент получает навык выявления: рисков цифровизации общества: в экономике, политике, образовании, медицине и других областях, связанных с человеком; роли человеческого фактора в информационной безопасности.</p> <p>2. Теоретические аспекты развития информационного общества. В результате выполнения практического задания студент получает навык анализа развития информационного общества и выявления закономерностей и особенностей распространения информации в виртуальном мире.</p> <p>3. Информационно-психологическое воздействие в международных отношениях и в масштабах защищаемой организации. В результате выполнения практического задания студент получает навыки анализа приемов выявления элементов Информационно-психологическое воздействие в международных отношениях и в масштабах защищаемой организации.</p> <p>4. Приемы психологического воздействия на личность и общество, способы защиты от манипулирования. В результате выполнения практического задания студент получает навыки владения приемами выявления приемов психологического воздействия и манипулирования и противодействия им в профессиональной деятельности.</p> <p>5. Информационная война и методы её ведения. Средства ведения информационных войн. В результате выполнения практического задания студент получает навыки выявления средств информационно-психологического оружия в СМИ и других информационных ресурсах.</p> <p>6. Информационные операции: понятие, виды, структура. Приемы информационного противоборства. В результате выполнения практического задания студент получает навык выявления приемов информационного противоборства в информационном пространстве.</p> <p>7. Человеческий фактор в вопросах обеспечения информационной безопасности. В результате выполнения практического задания студент получает навык выявления приемов манипулирования «социальных инженеров» для добывания конфиденциальной информации и разработки стратегий противоборства им.</p> <p>8. Вопросы ИБ в управлении персоналом. В результате выполнения практического задания студент получает навык проектирования обучающего занятия с персоналом организации по вопросам информационной безопасности с применением интерактивных технологий обучения.</p>

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Подготовка докладов и проектов на заданную тему.
2	Работа с лекционным материалом.
3	Подготовка к практическим занятиям

4	Подготовка к промежуточной аттестации.
5	Подготовка к текущему контролю.

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

№ п/п	Библиографическое описание	Место доступа
1	Постановление Правительства РФ от 15.04.2014 N 313 (ред. от 30.11.2019) "Об утверждении государственной программы Российской Федерации "Информационное общество"	http://www.consultant.ru/document/cons_doc_LAW_162184/ (дата обращения: 02.10.2022).- Текст электронный.
2	Постановление Правительства РФ от 02.03.2019 N 234 (ред. от 07.12.2019) "О системе управления реализацией национальной программы "Цифровая экономика Российской Федерации" (вместе с "Положением о системе управления реализацией национальной программы "Цифровая экономика Российской Федерации")	http://www.consultant.ru/document/cons_doc_LAW_319701/ (дата обращения: 02.10.2022).- Текст электронный.
3	Чугунов А.В. Социальная информатика : учебное пособие. Москва : Издательство Юрайт, 2020.	Библиотека РУТ, https://biblio-online.ru/bcode/451096 (дата обращения: 02.10.2022).- Текст электронный.
4	Бухарин, С. Н., Цыганов В. В. Методы и технологии информационных войн. Москва : Академический Проект, 2020.	Библиотека РУТ , https://e.lanbook.com/book/132794 (дата обращения: 02.10.2022).- Текст электронный.

5	Манойло А.В., Петренко А.И., Фролов Д.Б. Государственная информационная политика в условиях информационно-психологической войны. Москва : Горячая линия-Телеком, 2017.	Библиотека РУТ , https://e.lanbook.com/book/111080 (дата обращения: 02.10.2022).- Текст электронный.
6	Масалков А.С. Особенности киберпреступлений: инструменты нападения и защиты информации Москва : ДМК Пресс, 2018.	Библиотека РУТ , https://e.lanbook.com/book/105842 (дата обращения: 02.10.2022).- Текст электронный.
7	Федоров Д.Ю. Гуманитарные аспекты информационной безопасности. Конспект лекций. СПб: ГЭУ, 2013	Библиотека РУТ , http://pycode.ru/files/gaib.pdf (дата обращения: 02.10.2022).- Текст электронный.
8	Полевая М.В. Управление человеческими ресурсами в условиях глобальных изменений : монография Москва : Прометей, 2019.	Библиотека РУТ , https://e.lanbook.com/book/126740 (дата обращения: 02.10.2022).- Текст электронный.

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

<http://www.consultant.ru>

<https://e.lanbook.com>

<https://www.elibrary.ru>

<https://www.kaspersky.ru>

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

Microsoft Windows.

При организации обучения по дисциплине (модулю) с применением электронного обучения и дистанционных образовательных технологий необходим доступ каждого студента к информационным ресурсам – библиотечному фонду Университета, сетевым ресурсам и информационно-телекоммуникационной сети «Интернет».

В случае проведения занятий с применением электронного обучения и дистанционных образовательных технологий может потребоваться наличие следующего программного обеспечения (или их аналогов): ОС Windows, Microsoft Office, Интернет-браузер, Microsoft Teams и т.д.

В образовательном процессе, при проведении занятий с применением электронного обучения и дистанционных образовательных технологий, могут применяться следующие средства коммуникаций: ЭИОС РУТ(МИИТ), Microsoft Teams, электронная почта, скайп, Zoom, WhatsApp и т.п.

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

Учебная аудитория для проведения занятий лекционного типа, практических занятий, лабораторных работ

В случае проведения занятий с применением электронного обучения и дистанционных образовательных технологий необходимо наличие компьютерной техники, для организации коллективных и индивидуальных форм общения педагогических работников со студентами, посредством используемых средств коммуникации.

Допускается замена оборудования его виртуальными аналогами.

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:

Е.М. Шпагина

Согласовано:

Заведующий кафедрой ВССиИБ

Б.В. Желенков

Председатель учебно-методической
комиссии

Н.А. Клычева