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: 22.04.2024

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-12 - 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-психологическое воздействия при совершении информационных аттак; 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 3 з.е. (108

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	Семестр 1
Контактная работа при проведении учебных занятий (всего):	50	50
В том числе:		
Занятия лекционного типа	30	30
Занятия семинарского типа	20	20

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 58 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	Введению в дисциплину «Гуманитарные аспекты информационной безопасности» Рассматриваемые вопросы: -Методологические основы, цели и задачи дисциплины, связь с другими науками.
2	Введению в дисциплину «Гуманитарные аспекты информационной безопасности»(продолжение) Рассматриваемые вопросы: -Основное противоречие информационной безопасности личности. -Роль информации в жизни человека.
3	Рассматриваемые вопросы: Рассматриваемые вопросы:

№ п/п	Тематика лекционных занятий / краткое содержание
	-Информационные революции и развитие информационного общества. -Основные теории информации. -Информационные революции.
4	Теоретические аспекты развития информационного общества (продолжение) Теоретические аспекты развития информационного общества (продолжение)
5	Информационно-психологическое воздействие в международных отношениях и в масштабах защищаемой организации Рассматриваемые вопросы: -Психология воздействия и манипулирования. -Принципы психологического воздействия.
6	Информационно-психологическое воздействие в международных отношениях и в масштабах защищаемой организации(продолжение) -Понятие, виды, средства, субъекты и мишени информационно-психологического воздействия.
7	Приемы психологического воздействия на личность и общество, способы защиты от манипулирования Рассматриваемые вопросы: -Психологическое воздействие и манипуляции: сходство и различие. -Виды манипулирования. -Побуждение и принуждение: скрытое и тайное. -Манипулирование информацией.
8	Приемы психологического воздействия на личность и общество, способы защиты от манипулирования(продолжение) Рассматриваемые вопросы: -Манипулятивное воздействие. - Манипулятивные технологии. -Дезинформирование. - Пропаганда. -Способы защиты от манипуляций.
9	Информационная война и методы её ведения. Средства ведения информационных войн Рассматриваемые вопросы: -Понятие информационных войн, сущность и методы ведения в работах отечественных и зарубежных ученых. - Моральная, ментальная, физическая война.
10	Информационная война и методы её ведения. Средства ведения информационных войн(продолжение) Рассматриваемые вопросы: -Кибервойна: кибератака, кибероборона, киберразведка. Информационное оружие, его характеристики. -Средства информационно-психологического оружия: печатные материалы; -средства массовой информации.
11	Информационные операции: понятие, виды, структура. Приемы информационного противоборства Рассматриваемые вопросы: -Информационная операция: структура, мишени, этапы. -Пропаганда и контрпропаганда: понятие, виды, цели и мишени воздействия.

№ п/п	Тематика лекционных занятий / краткое содержание
12	Информационные операции: понятие, виды, структура. Приемы информационного противоборства(продолжение) Рассматриваемые вопросы: - Информационный вброс. Алгоритм построения. -Распознавание информационного вброса и меры противодействия и разоблачения.
13	Человеческий фактор в вопросах обеспечения информационной безопасности Рассматриваемые вопросы: -Понятие «человеческий фактор», учет его роли в обеспечении информационной безопасности организации.
14	Человеческий фактор в вопросах обеспечения информационной безопасности(продолжение) -Социально-психологическая характеристика внутреннего и внешнего нарушителя, использование методов «социальной инженерии» для получения информации ограниченного доступа. -Приемы противоборства методам «социальной инженерии».
15	Вопросы ИБ в управлении персоналом -Подбор персонала на должности, связанные с работой с информацией ограниченного доступа. -Приемы обучения сотрудников навыкам обеспечения информационной безопасности в организации.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
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.
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.
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.
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.
5	Информационная война и методы её ведения В результате выполнения практического задания студент получает навыки выявления выявления и анализа методов информационно-психологического оружия в СМИ и других информационных ресурсах.

№ п/п	Тематика практических занятий/краткое содержание
6	Средства ведения информационных войн В результате выполнения практического задания студент получает навыки выявления средств информационно-психологического оружия в СМИ и других информационных ресурсах.
7	Информационные операции: понятие, виды, структура. Приемы информационного противоборства В результате выполнения практического задания студент получает навык выявления приемов информационного противоборства в информационном пространстве.
8	Человеческий фактор в вопросах обеспечения информационной безопасности В результате выполнения практического задания студент получает навык выявления приемов манипулирования «социальных инженеров» для добывания конфиденциальной информации.
9	Выявление и противоборство методам «социальной социальной инженерии». В результате выполнения практического задания студент получает навык разработки стратегий противоборства методам социальной инженерии.
10	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.

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"	Доступ из справочно-правовой системы «КонсультантПлюс» URL: http://www.consultant.ru/document/cons_doc_LAW_162184/(дата обращения: 22.02.2024).- 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")	Доступ из справочно-правовой системы «КонсультантПлюс» URL: http://www.consultant.ru/document/cons_doc_LAW_319701/(дата обращения: 22.02.2024).- Текст электронный.
3	Чугунов А.В., Социальная информатика : учебное пособие. Москва : Издательство Юрайт, 2020.256 с. — ISBN 978-5-534-09010-9.	Библиотека РУТ,https://biblio-online.ru/bcode/451096(дата обращения:22.02.2024.- Текст электронный.
4	Бухарин С. Н., Цыганов В. В. Методы и технологии информационных войн. Москва : Академический Проект, 2020.—336 с. — ISBN 978-5-8291-3178-4	Библиотека РУТ ,https://e.lanbook.com/book/132794(дата обращения:22.02.2024).- 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.— 542 с. — ISBN 978-5-9912-0253-4	Библиотека РУТ ,https://e.lanbook.com/book/111080 (дата обращения: 22.02.2024).- Текст электронный.
6	МасалковА.С., Особенности киберпреступлений: инструменты нападения и защиты информации Москва : ДМК Пресс,	Библиотека РУТ ,https://e.lanbook.com/book/105842 (дата обращения: 22.02.2024).- Текст электронный.

	2018.— 226 с. — ISBN 978-5-97060-651-3	
7	Козырь Н. С,. Гуманитарные аспекты информационной безопасности : учебное пособие для вузов / Н. С. Козырь, Н. В. Седых. — Москва : Издательство Юрайт, 2024. — 170 с. — ISBN 978-5-534-17153-2.	Библиотека РУТ, https://urait.ru/bcode/544965 (дата обращения: 09.02.2024). - Текст электронный.
8	Кругликов В. Н. , Интерактивные образовательные технологии : учебник и практикум для вузов / В. Н. Кругликов, М. В. Оленникова. — 3-е изд., испр. и доп. — Москва : Издательство Юрайт, 2024. — 355 с. — ISBN 978-5-534-15331-6.	Библиотека РУТ , https://urait.ru/bcode/539080 (дата обращения: 09.02.2024).- Текст электронный.

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

Справочно-правовая система КонсультантПлюс [сайт]. — URL: http://www.consultant.ru

Элекиронно-библиотечная система «ЭБС Лань» [сайт]. — URL: https://e.lanbook.com

Научная электронная библиотека «eLIBRARY.RU» URL:https://www.elibrary.ru

Лаборатория Касперского [сайт]. — URL: https://www.kaspersky.ru

Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/544965.

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 проведении занятий с применением электронного обучения и дистанционных образовательных технологий может понадобиться 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 проведении 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:

заведующий кафедрой, доцент, к.н.
кафедры «Вычислительные системы,
сети и информационная
безопасность» Б.В. Желенков

Согласовано:

Заведующий кафедрой ВССиИБ Б.В. Желенков

Председатель учебно-методической
комиссии Н.А. Андриянова