МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
базового высшего образования
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

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-1 - Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их

значение для обеспечения объективных потребностей личности, общества и государства;

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

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 атак;
- и 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 №8
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	Введение в дисциплину. Актуальные проблемы ИБ, связанные с человеческим фактором. OSINT и HUMINT. Рассматриваемые вопросы: - Методологические основы, цели и задачи дисциплины, связь с другими науками. - Роль информации в жизни человека. Основное противоречие информационной безопасности личности. - Развитие методов OSINT и HUMINT в мировой практике получения информации ограниченного доступа.

№ п/п	Тематика лекционных занятий / краткое содержание
2	Теории информации. Рассматриваемые вопросы: - Влияние информации на человека и социальные процессы. - Эволюция создания информационного общества, цифровой экономики и цифровизации общественных процессов. - Социальные сети, их роль в развитии цифрового общества.
3	Человеческий фактор как уязвимость. Психология виктимности. Рассматриваемые вопросы: - Понятие человеческого фактора в психологии безопасности и его значение для информационной безопасности. - Основные понятия психологии виктимности: личностные и ситуационные факторы, превращающие человека в жертву или мишень воздействия правонарушителей.
4	Психология влияния и манипулирования. Основные приемы психологического воздействия. Рассматриваемые вопросы: - Основные универсальных психологические принципы влияния (взаимность, авторитет, социальное доказательство, дефицит, последовательность), которые манипуляторы используют для управления поведением и решениями людей; знание этих принципов для распознавания и нейтрализации манипуляции. - Отличие манипуляции от убеждения; этическая оценка последствий для благополучия человека. - Применение вербальных (фрейминг, вопросы-вилки, навешивание ярлыков, «якорение»), невербальные (мимика, поза, тон) и контекстуальные приёмов (создание дефицита, давление времени, социальные подсказки).
5	Продолжение Психология влияния и манипулирования. Основные приемы психологического воздействия. Рассматриваемые вопросы: - Личностные факторы (низкая самооценка, высокая тревожность, потребность в одобрении) и ситуационные стрессоры, определяющие уязвимость к воздействию. - Профилактика рисков манипуляции сознанием и поведением в контексте информационной безопасности.
6	Социальная инженерия. Методы социальной инженерии. Рассматриваемые вопросы: - Социальная инженерия: определение, исторические примеры и современные тренды в контексте информационной безопасности. - Основные категории атак социальной инженерии (фишинг, вишинг, смшинг, пре-текстинг, байпас доверия, физический доступ) и каков механизм их действия. - психологические приёмы и когнитивные искажения, которые используют злоумышленники (социальное доказательство, дефицит, авторитет, взаимность, спешка, эмоции) и как они работают в типичных сценариях атак.
7	Социальная инженерия. Методы социальной инженерии. Рассматриваемые вопросы: - Прямые методы социальной инженерия. - Обратные методы социальной инженерии. - Обнаружение и противодействие атакам социальной инженерии: практические методы обучения сотрудников (фишинг тесты, сценарные тренинги), инструменты мониторинга и реагирования, а также разработка политики реагирования и регулярной оценки эффективности.
8	Тактики и приемы нарушителей в получении конфиденциальной информации. Рассматриваемые вопросы: - Психологические приёмы (манипуляция эмоциями, давление времени, авторитет, взаимность, социальное доказательство), которые помогают злоумышленникам преодолевать сопротивление

№ п/п	Тематика лекционных занятий / краткое содержание
	людей и заставлять их раскрывать данные. - Роли и позиции сотрудников внутри организации наиболее уязвимы к целенаправленным атакам и почему (например, административный персонал, IT?поддержка, топ?менеджмент). - Технические и процедурные уязвимости (отсутствие контроля физического доступа, слабая аутентификация, недостаточно строгие регламенты обмена информацией), которые часто комбинируются с человеческим фактором в успешных атаках.
9	Методы противостояния вербовке. Рассматриваемые вопросы: - Понятие вербовки формы проявления: длительные манипуляции, внезапные предложения, «мягкая» радикализация или эксплуатация личных связей. - Этапы процесса вербовки (выявление, установление контакта, завоевание доверия, эксплуатация) и сигналы, которые могут указывать на попытку вербовки? - Личностные и ситуационные факторы, повышающие уязвимость сотрудника к вербовке (финансовые проблемы, неудовлетворённость работой, одиночество, амбиции, идеологическая симпатия) - Организационные меры и процедуры снижающие риск успешной вербовки (политики разграничения доступа, регулярные проверки благонадёжности, программы поддержки сотрудников).
10	Информационная война. Формы ведения информационной войны. Рассматриваемые вопросы: - Понятие «информационная война»: цели, субъекты (государства, негосударственные акторы), и отличие от пропаганды и кибероперaций. - Формы ведения информационной войны (публичная пропаганда, дезинформация и фейковые новости, психологические операции, информационно?психологическое воздействие на население, влияние через социальные сети и платформы) и их особенности.
11	Информационная война. Формы ведения информационной войны. Рассматриваемые вопросы: - Новые риски современных цифровых инструментов и техник (бот сети, таргетированная реклама, генеративный ИИ, deepfake, микротаргетинг) для реализации информационных кампаний в ходе ведения информационных войн. -Тактические приёмы информационных операций в ходе информационной войны.
12	Методы противоборства в информационной войне. Рассматриваемые вопросы: - Стратегические уровни противоборства в информационной войне существуют (превентивный, оперативный, стратегический); задачи, решаемые на каждом уровне. -Инструменты государственного и общественного реагирования против дезинформации и враждебных информационных кампаний (медиаграмотность, фактчекинг, контрнарративы, правовое регулирование, сотрудничество с платформами). - Технические методы (детекция ботов и фейковых аккаунтов, анализ сетевых паттернов, использование ИИ для мониторинга нарративов, фильтрация контента), сочетаемые с организационными и педагогическими мерами для снижения влияния враждебной информации. - Этические и правовые ограничения при реализации мер противодействия (цензура vs. свобода слова, приватность, прозрачность модерации): баланс между безопасностью и правами граждан.
13	Проблемы внедрения ИИ в различные сферы общественной жизни в контексте информационной безопасности Рассматриваемые вопросы: - Новые угрозы приватности. Массовое применение ИИ для анализа данных (распознавание,

№ п/п	Тематика лекционных занятий / краткое содержание
	предиктивная аналитика, профилирование) увеличивает риски нарушения конфиденциальности и несанкционированного использования персональных данных, особенно в условиях слабого регулирования и отсутствия единых стандартов защиты. - Генеративные фейки и deepfake. ИИ-генераторы контента (текст, изображение, аудио, видео) делают создание убедительных фейков и подделок доступным для широкого круга злоумышленников, что осложняет проверку аутентичности информации и усиливает дезинформацию в медиа и соцсетях. - Автоматизация кибератак: применение ИИ злоумышленниками для автоматизации эксплойтов, генерации сообщений, поиска уязвимостей и адаптации методов атак, что повышает скорость и масштаб ущерба для информационных систем. - Уязвимости ИИ-моделей: сами ИИ-системы подвержены атакам (вредоносные входные данные, training poisoning, adversarial примеры, извлечение моделей), что создаёт риски необоснованных решений, подмены классификаций и компрометации критических процессов.
14	Работа с персоналом организации по обучению основам информационной безопасности. Рассматриваемые вопросы: - Цели и задачи обучения персонала основам информационной безопасности в организации и как их соотносить с требованиями к защите информации ограниченного доступа. - Форматы и методы обучения для разных категорий сотрудников (очные тренинги, онлайн-курсы, симуляции фишинга, сценарные упражнения, регулярные встречи) и оценка их результативность. - Методы диагностики надёжности персонала применяются для допуска к информации ограниченного доступа (проверка благонадёжности, биографический опрос, полиграф, психологическое тестирование, референс-чеки, анализ социальных связей) и какие их сильные/слабые стороны.
15	Работа с персоналом организации по обучению основам информационной безопасности. Рассматриваемые вопросы: - Интерактивные методы обучения персонала информационной безопасности. -Метод правого дизайна в обучении - Мониторинг и повторная оценка надёжности персонала после допуска (периодические проверки, анализ поведения и инцидентов, каналы анонимного сообщения о подозрительных фактах). Интеграция результатов диагностики и обучения в систему управления рисками ИБ персонала информационной безопасности.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Введение в дисциплину. Актуальные проблемы ИБ, связанные с человеческим фактором. OSINT и HUMINT 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	Человеческий фактор как уязвимость. Психология виктимности. В результате выполнения практического задания студент получает навык выявления мишени воздействия правонарушителей на слабые места личности; понимания состояний и ситуаций,

№ п/п	Тематика практических занятий/краткое содержание
	способствующих виктимности; анализировать реальные или смоделированные случаи атак, использовать теорию для объяснения механизмов воздействия и предложить обоснованные меры противодействия с учётом психологических факторов.
3	Психология влияния и манипулирования. Основные приемы психологического воздействия. В результате выполнения практического задания студент получает навык понимания психологических принципов влияния (взаимность, авторитет, социальное доказательство, дефицит, последовательность, симпатия) и приводить примеры их применения в реальных ситуациях. Различать этику и механизмы убеждения и манипуляции, определять, когда воздействие становится манипулятивным (скрытые мотивы, использование уязвимостей, отсутствие добровольного информированного согласия), идентифицировать вербальные и невербальные приёмы манипуляции (фрейминг, вопросы-вилки, якорение, подстройка, работа с эмоциями, создание ощущения спешки) и описывать механизм их действия.
4	Социальная инженерия. Методы социальной инженерии. В результате выполнения практического задания студент получает навык диагностики и выявления методов и приемов социальной инженерии; навык разработки стратегий противоборства методам и приемам социальной инженерии.
5	Тактики и приемы нарушителей в получении конфиденциальной информации. В результате выполнения практического задания студент получает навык называть и описывать основные тактики внешних нарушителей (фишинг, вишинг, смшинг, пре?текстинг, baiting, quid pro quo, бюджетирование доверия, создание ложного авторитета) и объяснять, как каждая из них работает в реальных атаках; студент способен объяснить, какие психологические принципы (взаимность, авторитет, социальное доказательство, дефицит, симпатия, спешка, эмоциональное давление) нарушители используют для преодоления сопротивления жертв и получения конфиденциальной информации; применять полученные знания в смоделированных ситуациях: распознавать признаки атаки, использовать техники «паузы» и проверки, задавать уточняющие вопросы, обращаться к службе безопасности, фиксировать инциденты и действовать по установленным процедурам реагирования.
6	Методы противостояния вербовке. В результате выполнения практического задания студент получает навык выявлять ранние сигналы и характерные черты попыток вербовки (внезапные «удобные» предложения, чрезмерное внимание, давление на личные проблемы, использование тайны, попытки установить доверительные отношения, предложение выгоды в обмен на информацию) и отличать их от обычных профессиональных контактов; определять личные и ситуационные факторы, повышающие риск вербовки (финансовые проблемы, неудовлетворённость работой, одиночество, амбиции, идеологическая симпатия, низкая осведомлённость о рисках) и предлагать способы их снижения; применять практические техники защиты: критическое оценивание предложений, использование «паузы» перед ответом, проверка фактов и источников, запрос второй точки зрения, отказ от обсуждения конфиденциальной информации, обращение к службе безопасности, фиксация контактов и сообщений.
7	Информационная война. Формы ведения информационной войны. В результате выполнения практического задания студент получает навык идентификации форм и методов ведения информационной войны (публичная пропаганда, дезинформация и фейковые новости, психологические операции, информационно?психологическое воздействие на население, влияние через социальные сети и платформы) и приводить примеры их применения; уметь оценивать современные технологии (бот?сети, таргетированная реклама, генеративный ИИ, deepfake, микротаргетинг) используемые для реализации информационных кампаний, и объяснять, какие новые риски они создают для общества и государства; выделять этапы информационной кампании (подготовка контекста, запуск нарратива, эскалация, прикрытие и поддержание), описать используемые тактические приёмы и проанализировать иллюстративные сценарии.

№ п/п	Тематика практических занятий/краткое содержание
8	Методы противоборства в информационной войне. В результате выполнения практического задания студент получает навык различения стратегических уровней противоборства существуют (превентивный, оперативный, стратегический); сравнить эффективные инструменты противодействия дезинформации и враждебным информационным кампаниям (медиаграмотность, фактчекинг, контрнарративы, правовое регулирование, сотрудничество с платформами, международная координация) и приводить примеры их применения; подбирать технические решения для обнаружения враждебной информации (детекция ботов и фейковых аккаунтов, анализ сетевых паттернов, применение ИИ для мониторинга нарративов, фильтрация контента), и объяснять их роль в сочетании с организационными и педагогическими мерами.
9	Проблемы внедрения ИИ в различные сферы общественной жизни в контексте информационной безопасности В результате выполнения практического задания студент получает навык выявления рисков информационной безопасности из-за внедрения ИИ с учетом этических и правовых норм; оценивать риски ИИ-систем на всех этапах жизненного цикла для исключения причинения вреда и уязвимости перед кибератаками; обеспечивать информационную безопасность цифровой среды, формируя и защищая цифровую репутацию$
10	Работа с персоналом организации по обучению основам информационной безопасности/ 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	Гуманитарные аспекты информационной безопасности : учебное пособие / В. В. Золотарев, Е. А. Маро, Н. Ю. Паротькин, П. А. Звягинцева. — Красноярск : СибГУ им. академика М. Ф. Решетнёва, 2023. — 78 с. — Текст : электронный // Лань : электронно-библиотечная система.	https://e.lanbook.com/book/400568(дата обращения: 12.03.2026)

2	Чудинов, С. И. Гуманитарные аспекты информационной безопасности : учебное пособие / С. И. Чудинов. — Новосибирск : СГУГиТ, 2021. — 44 с. — ISBN 978-5-907320-85-7. — Текст : электронный // Лань : электронно-библиотечная система.	https://e.lanbook.com/book/222341(дата обращения: 12.03.2026)
3	Гуманитарные аспекты информационной безопасности: практикум для студентов, обучающихся по программам бакалавриата всех направлений и профилей : учебное пособие / составитель Л. А. Коноплева. — Екатеринбург :УрГЭУ, 2023. — 106 с. — Текст : электронный //Лань : электронно-библиотечная система.	https://e.lanbook.com/book/406781(дата обращения: 12.03.2026)
4	Романов, В. Г. Социальная инженерия мошенничества : монография / В. Г. Романов, И. В. Романова. — Чита : ЗабГУ, 2021. — 240 с. — ISBN 978-5-9293-2771-1. — Текст : электронный // Лань : электронно-библиотечная система.	https://e.lanbook.com/book/271808 (дата обращения: 12.03.2026)
5	Манойло, А. В. Государственная информационная политика в условиях информационно-психологической войны / А. В. Манойло, А. И. Петренко, Д. Б. Фролов. — 3-е изд., стер. — Москва : Горячая линия-Телеком, 2017. — 542 с. — ISBN 978-5-9912-0253-4. — Текст : электронный // Лань : электронно-библиотечная система.	https://e.lanbook.com/book/111080(дата обращения: 12.03.2026)
6	Психология влияния и манипуляций : учебное пособие / составитель Л. С. Самсоненко. — Оренбург : ОГПУ, 2022. — 70 с. — Текст : электронный // Лань : электронно-библиотечная система.	https://e.lanbook.com/book/239615(дата обращения: 12.03.2026)

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

Электронно-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).

ОС Windows
- Microsoft Office
- Foxit Reader/Acrobat Reader
- Интернет-браузер (Yandex и др.)

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

Учебная аудитория для проведения учебных занятий (занятий лекционного типа, практических занятий):

- компьютер преподавателя, рабочие станции студентов, мультимедийное оборудование, доска.

Аудитория подключена к сети «Интернет».

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. Андриянова