Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Структурное подразделение «Институт информационных технологий и анализа данных (121)»

УТВЕРЖДЕНА:
на заседании совета института ИТиАД им. Е.И. Попова
Протокол №8 от 16 февраля 2026 г.

Рабочая программа дисциплины

«СОЦИАЛЬНЫЕ ТЕХНОЛОГИИ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление: 10.03.01 Информационная безопасность

Организация и технологии защиты информации (в сфере техники и технологии)

Квалификация: Бакалавр

Форма обучения: очная

Документ подписан простой электронной подписью Составитель программы: Ларионова Лариса Александровна Дата подписания: 17.06.2026	Документ подписан простой электронной подписью Утвердил: Говорков Алексей Сергеевич Дата подписания: 17.06.2026	Документ подписан простой электронной подписью Согласовал: Маринов Александр Андреевич Дата подписания: 17.06.2026

Год набора – 2026

Иркутск, 2026 г.

1 Перечень планируемых результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы

1.1 Дисциплина «Социальные технологии в информационной безопасности» обеспечивает формирование следующих компетенций с учётом индикаторов их достижения

Код, наименование компетенции	Код индикатора компетенции
ДК-1 Способность осуществлять деятельность, находящуюся за пределами основной профессиональной сферы	ДК-1.3

1.2 В результате освоения дисциплины у обучающихся должны быть сформированы

Код индикатора	Содержание индикатора	Результат обучения
ДК-1.3	Способен применять в сфере социального обеспечения технологии ИИ для улучшения обслуживания пользователей в режиме онлайн, внедрения технологии интеллектуальных чат-ботов в социотехнические системы, а также применять профессиональные решения с целью предотвращения утечки конфиденциальной информации	**Знать** основные принципы работы технологий искусственного интеллекта и их применение в сфере социального обеспечения; законодательство и этические нормы, касающиеся обработки персональных данных и конфиденциальной информации; различные типы интеллектуальных чат-ботов и их функциональные возможности; принципы проектирования социотехнических систем и их компонентов. **Уметь** оценивать риски утечки конфиденциальной информации и разрабатывать меры по их предотвращению; использовать инструменты и платформы для интеграции ИИ в существующие социотехнические системы. **Владеть** 1. Навыками работы с программным обеспечением для разработки и управления чат-ботами. 2. Компетенциями в области анализа данных для оценки эффективности внедренных технологий. 3. Знаниями в области кибербезопасности и защиты данных. 4. Умением взаимодействовать с

		многопрофильными командами для успешной реализации проектов по внедрению ИИ.

2 Место дисциплины в структуре ООП

Изучение дисциплины «Социальные технологии в информационной безопасности» базируется на результатах освоения следующих дисциплин/практик: «Информационно-психологическая безопасность в современном обществе», «Искусственный интеллект»

Дисциплина является предшествующей для дисциплин/практик: «Производственная практика: преддипломная практика»

3 Объем дисциплины

Объем дисциплины составляет – 3 ЗЕТ

Вид учебной работы	**Трудоемкость в академических часах** (Один академический час соответствует 45 минутам астрономического часа)	
	Всего	Семестр № 7
Общая трудоемкость дисциплины	108	108
Аудиторные занятия, в том числе:	48	48
лекции	32	32
лабораторные работы	0	0
практические/семинарские занятия	16	16
Самостоятельная работа (в т.ч. курсовое проектирование)	60	60
Трудоемкость промежуточной аттестации	0	0
Вид промежуточной аттестации (итогового контроля по дисциплине)	Зачет	Зачет

4 Структура и содержание дисциплины

4.1 Сводные данные по содержанию дисциплины

Семестр № 7

№ п/п	**Наименование раздела и темы дисциплины**	**Виды контактной работы**						СРС		**Форма текущего контроля**
		Лекции		ЛР		ПЗ(СЕМ)				
		№	Кол. Час.	№	Кол. Час.	№	Кол. Час.	№	Кол. Час.	
1	2	3	4	5	6	7	8	9	10	11
1	Социальная инженерия как деструктивная технология в контексте информационной безопасности	1	4			1	2	1	7	Устный опрос
2	Социальная инженерия как инструмент атак на цифровую							1	6	Устный опрос

	личность									
3	Психические и ментальные вирусы	2	4			2	2	1	7	Устный опрос
4	Аналитика больших данных							1	7	Устный опрос
5	Технологии защиты цифровой идентичности	3	4			3	2			Устный опрос
6	Противодействие информационно-психологическим операциям (ИПО) в контексте цифровой личности									Устный опрос
7	Социально-психологические барьеры переработки информации	4	4			4	2	1	7	Устный опрос
8	Противодействия информационно-психологическим операциям	5	4			5	2	1	7	Устный опрос
9	Киберфизические системы, проблемы проектирования киберфизических систем	6	3			6	1	1	7	Устный опрос
10	Цифровая гигиена и управление цифровой репутацией	7	3			7	1	1	6	Устный опрос
11	Стандарт Essence в системной инженерии	8	3			8	2	1	6	Устный опрос
12	Метод ARCADIA и инструментальное средство Capella.	9	3			9	2			Устный опрос
	Промежуточная аттестация									Зачет
	Всего		32				16		60	

4.2 **Краткое содержание разделов и тем занятий**

Семестр № 7

№	Тема	Краткое содержание
1	Социальная инженерия как деструктивная технология в контексте информационной безопасности	Использование психологических методов и способов получения доступа к информации в результате атак и мошеннических схем. Психологическая сущность претекстинга. Социальные информационные технологии как рычаг управления человеком. Психотропный террор. Киберэкстремизм.

2	Социальная инженерия как инструмент атак на цифровую личность	Определение цифровой личности (Digital Identity). Компоненты: биометрические данные, поведенческие паттерны, цифровой след (Digital Shadow), репутационные активы. Цифровая личность как новый объект атак и предмет коммерциализации. Эволюция методов социальной инженерии от фишинга до дипфейков. Использование OSINT (разведки по открытым источникам) для сбора данных о цифровой личности. Клонирование личности с помощью генеративных нейросетей. Претекстинг и психологические манипуляции для получения биометрических и персональных данных.
3	Психические и ментальные вирусы	Внутреннее отображение информации в сознании. Средства «перепрошивки» сознания человека. Механизмы воздействия вирусов. Проектные вирусы. Макиавеллизм. Меметика.
4	Аналитика больших данных	Визуализация. Когнитивные схемы. Машинное обучение. KDD, Data Mining, Text Mining. Контент-мониторинг и контент-анализ. Интегрированные системы разведки. Метапоиск
5	Технологии защиты цифровой идентичности	Многофакторная аутентификация как краеугольный камень защиты цифровой личности. Биометрическая защита и уязвимости биометрии перед социальной инженерией. Управление паролями и использование менеджеров паролей. Принципы работы с электронной подписью, электронным штампом времени и eID.
6	Противодействие информационно-психологическим операциям (ИПО) в контексте цифровой личности	Когнитивные технологии как инструмент сетевых войн. Защита от информационного вандализма и киберсталкинга. Моделирование процессов противодействия атакам на цифровую личность. Правовые и этические аспекты защиты персональных данных (ФЗ-152).
7	Социально-психологические барьеры переработки информации	Искажение передачи и восприятия информации. Упрощенные схемы мышления. Эвристические правила. Ошибки нарратива.
8	Противодействия информационно-психологическим операциям	Когнитивные технологии как инструмент сетевых войн. Противодействие информационному вандализму, криминалу и терроризму. Когнитивно-аксиологическая концепция общественной безопасности. Социально-психологические и когнитивные аспекты обеспечения национальной безопасности. Моделирование процессов противодействия информационно-психологическим операциям. Модель анализа рисков. Динамическая модель противоборства.
9	Киберфизические системы, проблемы	Разнообразие областей применения КФС делает востребованным качественно новый по сложности

	проектирования киберфизических систем	уровень автоматизации, позволяющий проектировать и массово производить системы, которые иначе было бы невозможно создать в принципе (например, беспилотные автомобили). В таких, на первый взгляд, далеких от компьютеров системах вычислительная компонента начинает играть ведущую роль, а обязанности ИТ-специалиста расширяются до полноценного системного инженера. Сегодня реализация сбалансированного киберфизического подхода остается скорее искусством, чем отработанной технологией. Существующие методики и маршруты проектирования тяготеют либо к «физико-центричному», либо к «компьютеро-центричному» подходу.
10	Цифровая гигиена и управление цифровой репутацией	Правила цифровой гигиены для минимизации цифрового следа. Управление настройками приватности в социальных сетях. Стратегии защиты цифровой репутации. Роль человеческого фактора и культуры безопасности в организациях.
11	Стандарт Essence в системной инженерии	Essence представляет собой методологическое ядро и язык для описания, создания, использования на практике и улучшения методов программной инженерии. Стандарт Essence, при минимальных изменениях, может использоваться также и в более широком смысле – в области системной инженерии, в том числе и при создании КФС. Суть подхода Essence можно прояснить с помощью так называемой «архитектуры метода».
12	Метод ARCADIA и инструментальное средство Capella.	С помощью ARCADIA/Capella можно провести моделирование архитектуры будущей системы и на ранних этапах отследить возможность выполнения функциональных и нефункциональных требований. Метод ARCADIA представляет систему в виде набора связанных между собой моделей на разных уровнях абстракции и позволяет анализировать её с разных точек зрения, рассматривая каждый значимый аспект проектирования.

4.3 Перечень лабораторных работ

Лабораторных работ не предусмотрено

4.4 Перечень практических занятий

Семестр № 7

№	Темы практических (семинарских) занятий	Кол-во академических часов
1	Социальная инженерия как деструктивная технология в контексте информационной	2

	безопасности	
2	Психические и ментальные вирусы	2
3	Аналитика больших данных	2
4	Социально-психологические барьеры переработки информации	2
5	Противодействия информационно-психологическим операциям	2
6	Киберфизические системы, проблемы проектирования киберфизических систем	1
7	Подготовка специалистов для проектирования киберфизических систем	1
8	Стандарт Essence в системной инженерии	2
9	Метод ARCADIA и инструментальное средство Capella	2

4.5 Самостоятельная работа

Семестр № 7

№	Вид СРС	Кол-во академических часов
1	Подготовка к практическим занятиям	60

В ходе проведения занятий по дисциплине используются следующие интерактивные методы обучения: интерактивная лекция, кейс-стади, дискуссия

5 Перечень учебно-методического обеспечения дисциплины

5.1 Методические указания для обучающихся по освоению дисциплины

5.1.1 Методические указания для обучающихся по практическим занятиям

https://el.istu.edu/enrol/index.php?id=7981

5.1.2 Методические указания для обучающихся по самостоятельной работе:

https://el.istu.edu/enrol/index.php?id=7981

6 Фонд оценочных средств для контроля текущей успеваемости и проведения промежуточной аттестации по дисциплине

6.1 Оценочные средства для проведения текущего контроля

6.1.1 семестр 7 | Устный опрос

Описание процедуры.

Проведение устного опроса в форме «вопрос-ответ».
Устный опрос проводится по окончанию лекционных занятий путем опроса студентов по списочному составу (при наличии бюджета времени после обсуждения установленных вопросов).

Критерии оценивания.

ответ раскрыт полностью 8-10 баллов
ответ раскрыт частично 4-7 баллов
имеет только общее представление о проблеме 2-4 баллов
не ответил – 0 баллов

6.2 Оценочные средства для проведения промежуточной аттестации

6.2.1 Критерии и средства (методы) оценивания индикаторов достижения компетенции в рамках промежуточной аттестации

Индикатор достижения компетенции	Критерии оценивания	Средства (методы) оценивания промежуточной аттестации
ДК-1.3	Способен продемонстрировать знания в сфере социальных аспектов применения информационных технологии. Правильно применяет профессиональные решения с целью предотвращения утечки конфиденциальной информации.	Устное собеседование по теоретическим вопросам, практико-ориентированные задания, дискуссия

6.2.2 Типовые оценочные средства промежуточной аттестации

6.2.2.1 Семестр 7, Типовые оценочные средства для проведения зачета по дисциплине

6.2.2.1.1 Описание процедуры

1) Зачет по дисциплине проводится согласно расписанию в назначенной аудитории, в которую приглашается к установленному началу экзамена группа студентов.
2) К зачету допускаются студенты, которые выполнили все предусмотренные работы по освоению курса: сданы практические работы по выбранной теме.
3). Каждый студент из числа допущенных выбирает один билет и готовится к ответу в течение не менее 30 - 45 минут письменно на поставленные три вопроса в билете.
Зачет проводится в форме устного опроса по билетам.

1. Особенности воздействия информационного пространства в современном обществе.
2. Культура кибербезопасности личности.
3. Методы социальной инженерии в информационно-психологическом пространстве.
4. Психологический анализ и оценка контента в системе OSINT.
5. Понятие о профайлинге.
6. Особенности поведения людей в ситуации опасности.
7. Факторы и причины угроз психологической безопасности человека.
8. Модели сенсорного восприятия информации (Д.Бродбент).
9. Методология когнитивного моделирования – способы мышления человека в условиях неопределенности (Р.Аксельрод).
10. Особенности мышления человека. Структура мышления. Критичность мышления. Клиповое мышление как риск нарушения безопасности (Э.Тоффлер).
11. Когнитивные ошибки (иррациональное мышление) как риск низкой

самоэффективности (А.Бек, А.Эллис).
12. Копинг-стратегии в неустойчивых эмоциональных состояниях (стресс, тревога, депрессия).
13. Синдром упущенной выгоды (FOMO).
14. Уровни удовлетворенности жизнью. Уровни доверия.
15. Виртуализация сеттинга.
16. Типология жертв киберпреступлений.
17. Прямое и косвенное воздействие на психику человека.
18. Донаучные школы воздействия на человека: Животный магнетизм (Ф.А. Месмер).
19. Использование методов месмеризма в информационном пространстве нового времени (XX в.). Магнетический транс (Д.Брейд).
20. Школы гипноза. Модель гипноза М.Эриксона. Методы нейролингвистического программирования (Р.Бендлер и Д.Гриндер).
21. Интегративная модель воздействия на человека в современном киберпространстве.
22. Психологическая устойчивость как стратегия формирования психологической безопасности.
23. Факторы и условия формирования психологической устойчивости.
24. Копинг-стратегии как актуальные ответы личности на воспринимаемую угрозу, их виды.
25. Формирование компонентов структурно-функциональной системы личности: мировоззренческие, мыслительные, эмоциональные, волевые.
26. Разновидности психологической защиты. Характеристики психологических защит. Система защитных мер в психологическом информационном пространстве.

6.2.2.1.2 Критерии оценивания

Зачтено	Не зачтено
Допускает незначительные ошибки в ответе на один из вопросов, включая дополнительные по результатам собеседования	Не отвечает на два и более вопросов

7 Основная учебная литература

1. Семенова Е. А. Социальная психология : учебное пособие / Е. А. Семенова, 2007. - 100.

[Сайт] – URL: http://elib.istu.edu/viewer/view.php?file=/files3/er-24524.pdf

8 Дополнительная учебная литература и справочная

1. Солсо Роберт Л. Когнитивная психология : [Пер. с англ.] / Роберт Л. Солсо, 2002. - 598.

2. Столяренко Л. Д. Основы психологии в экзаменационных вопросах и ответах : учеб. пособие / Л. Д. Столяренко, 2003. - 443.

3. Ахмедов Т. И. Практическая психотерапия: внушение, гипноз, медитация : монография / Тариэл Ахмедов, 2005. - 447.

4. Эриксон Бетти Элис. Семинар с Бетти Элис Эриксон: новые уроки гипноза / Бетти Элис Эриксон; Под ред. М. Р. Гинзбурга, 2002. - 203.

9 Ресурсы сети Интернет

1. http://library.istu.edu/
2. https://e.lanbook.com/

10 Профессиональные базы данных

1. http://new.fips.ru/
2. http://www1.fips.ru/

11 Перечень информационных технологий, лицензионных и свободно распространяемых специализированных программных средств, информационных справочных систем

1. Свободно распространяемое программное обеспечение Microsoft Windows Seven Professional (Microsoft Windows Seven Starter) - Seven, Vista, XP_prof_64, XP_prof_32 - поставка 2010

2. Свободно распространяемое программное обеспечение Microsoft Windows Seven Professional [1x100] RUS (проведен апгрейд с Microsoft Windows Seven Starter [1x100]) - поставка 2010

3. Свободно распространяемое программное обеспечение Microsoft Windows Server Standard 2008 R2 Russian Academic OPEN 1 License No Level

12 Материально-техническое обеспечение дисциплины

1. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

2. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

3. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

4. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

5. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

6. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

7. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

8. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

9. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

10. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

11. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

12. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

13. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

14. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

15. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

16. МФУ FS-1128 MFP

17. Сервер CPU Intel Core i7-960/GA-X58A-UD3R/DDR-IIIDimm 2Gb/HDD 1 Tb/DVD-RW/512MB PCI-E/блок пит.+ПО

18. Проектор Epson EB-W04LCD.WXGA 1280*800.3000:1.2800 ANSI Lumens