Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Структурное подразделение «Истории и философии»

УТВЕРЖДЕНА:
на заседании кафедры
Протокол №4 от 04 февраля 2025 г.

Рабочая программа дисциплины

«ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ В СОВРЕМЕННОМ ОБЩЕСТВЕ»

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: 30.05.2025	Документ подписан простой электронной подписью Утвердил: Новиков Павел Александрович Дата подписания: 17.06.2025	Документ подписан простой электронной подписью Согласовал: Сибиряк Юрий Владимирович Дата подписания: 02.06.2025

Год набора – 2025

Иркутск, 2025 г.

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

1.1 Дисциплина «Информационно-психологическая безопасность в современном обществе» обеспечивает формирование следующих компетенций с учётом индикаторов их достижения

Код, наименование компетенции	Код индикатора компетенции
ПКС-1 Способность анализировать функциональный процесс объекта информатизации, включая социотехнические системы с применением программных средств для определения возможных источников информационных угроз, их вероятных целей и тактики; организовывать и сопровождать аттестацию объекта защиты в соответствии с требованиями безопасности информации	ПКС-1.2

1.2 В результате освоения дисциплины у обучающихся должны быть сформированы

Код индикатора	Содержание индикатора	Результат обучения
ПКС-1.2	Проводит совместный анализ для выявления возможных источников информационных угроз; умеет контролировать события безопасности и действия пользователей автоматизированных систем, применять нормативные документы по противодействию технической разведке; владеет методиками определения возможных информационно-психологических воздействий на пользователей, с целью предотвращения утечки конфиденциальной информации, в том числе ПНд	**Знать** теоретические основы и прикладные исследования в области обеспечения информационно-психологической безопасности в современном обществе, в том числе, принципы управления психологическими состояниями в ситуации информационно-психологического воздействия, способы противостояния личности деструктивному влиянию информационно-психологическому воздействию **Уметь** выявлять риски деструктивного информационно-психологического воздействия на психологические состояния личности, контролировать состояние собственной безопасности и безопасности в группе **Владеть** методами и методиками выявления деструктивных факторов информационно-психологического воздействия на личность и группу, способами регуляции собственными состояниями, способами эффективного взаимодействия в социальной среде для предупреждения деструктивного

		информационно-психологического воздействия на личность и/или группу

2 Место дисциплины в структуре ООП

Изучение дисциплины «Информационно-психологическая безопасность в современном обществе» базируется на результатах освоения следующих дисциплин/практик: «Введение в профессиональную деятельность», «Критическое и системное мышление»

Дисциплина является предшествующей для дисциплин/практик: «Безопасность операционных систем», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», «Социальные технологии в информационной безопасности»

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 № 4
Общая трудоемкость дисциплины	108	108
Аудиторные занятия, в том числе:	64	64
лекции	32	32
лабораторные работы	0	0
практические/семинарские занятия	32	32
Самостоятельная работа (в т.ч. курсовое проектирование)	44	44
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 № 4

№ 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	Человеческий фактор в информационно-психологической безопасности в современном обществе	1	7			1, 2	7	1, 2, 2, 3, 3	21	Устный опрос
2	Когнитивный аспект	2	7			3, 4, 5	7	1, 2, 3	12	Устный опрос

	кибербезопасности									
3	Кибервиктимность: факторы, формирующие виктимное поведение	3	6			6, 7	6	1, 2	5	Творческое задание
4	Методы и средства воздействия на человека	4	6			8, 9	6	1	2	Устный опрос
5	Стратегии и механизмы формирования психологической безопасности личности в киберпространстве	5	6			10, 11	6	1, 2	4	Собеседование
	Промежуточная аттестация									Зачет
	Всего		32				32		44	

4.2 **Краткое содержание разделов и тем занятий**

Семестр № 4

№	Тема	Краткое содержание
1	Человеческий фактор в информационно-психологической безопасности в современном обществе	Особенности воздействия информационного пространства в современном обществе. Культура кибербезопасности личности. Методы социальной инженерии в информационно-психологическом пространстве. Фишинг, вишинг, смишинг. Психологический анализ и оценка контента в технологии OSINT. Особенности поведения людей в ситуации опасности. Факторы и причины угроз психологической безопасности человека.
2	Когнитивный аспект кибербезопасности	Модели сенсорного восприятия информации (Д.Бродбент). Методология когнитивного моделирования – способы мышления человека в условиях неопределенности (Р.Аксельрод). Особенности мышления человека. Структура мышления. Критичность мышления. Клиповое мышление как риск нарушения безопасности (Э.Тоффлер). Когнитивное искажение информации и когнитивные ошибки в суждении о мире (иррациональное мышление) как риск низкой самоэффективности (А.Бек, А.Эллис). Ложь, фейки, дипфейки. Ментальный и психические вирусы. Меметика.
3	Кибервиктимность: факторы, формирующие виктимное поведение	Виктимность. Особенности кибервиктимности. Типы атак на человека в киберпространстве: кибербуллинг, киберсталкинг, кибершейминг, кибертроллинг, газлайтинг. Копинг-стратегии в неустойчивых эмоциональных состояниях (стресс,

		тревога, депрессия). Синдром упущенной выгоды (FOMO). Уровни удовлетворенности жизнью. Уровни доверия. Виртуализация сеттинга. Типология жертв киберпреступлений.
4	Методы и средства воздействия на человека	Психологические основы манипулирования сознанием. Феномен скрытого управления человеком. Прямое и косвенное воздействие на психику человека. Донаучные школы воздействия на человека: Животный магнетизм (Ф.А. Месмер). Использование методов месмеризма в информационном пространстве нового времени (XX в.). Магнетический транс (Д.Брейд). Школы гипноза. Модель гипноза М.Эриксона. Методы нейролингвистического программирования (Р.Бендлер и Д.Гриндер). Подача информационного материала как способ воздействия. Использование шок-контента. Влияние виртуальной реальности на сознание. Интегративная модель воздействия на человека в современном киберпространстве.
5	Стратегии и механизмы формирования психологической безопасности личности в киберпространстве	Психологическая устойчивость как стратегия формирования психологической безопасности. Факторы и условия формирования психологической устойчивости. Копинг-стратегии как актуальные ответы личности на воспринимаемую угрозу, их виды. Формирование компонентов структурно-функциональной системы личности: мировоззренческие, мыслительные, эмоциональные, волевые. Разновидности психологической защиты. Характеристики психологических защит. Система защитных мер в психологическом информационном пространстве. Психологический аспект противодействия телефонному мошенничеству. Рефлексия, саморегуляция, индивидуальная траектория психологической защиты в киберпространстве.

4.3 Перечень лабораторных работ

Лабораторных работ не предусмотрено

4.4 Перечень практических занятий

Семестр № 4

№	Темы практических (семинарских) занятий	Кол-во академических часов
1	Особенности воздействия информационного пространства на человека в современном обществе.	4
2	Факторы и причины угроз психологической	3

	безопасности человека.	
3	Когнитивное искажение информации. Ложь, фейки, дипфейки	3
4	Ментальный и психический вирус. Меметика.	2
5	Иррациональное установки мышления как риск ошибочного восприятия информации	2
6	Виды атак на человека. Профайлинг виктима.	3
7	Типология жертв киберпреступлений	3
8	Влияние виртуальной реальности на сознание человека.	4
9	Интегративная модель воздействия на человека в современном киберпространстве.	2
10	Факторы и условия формирования психологической устойчивости.	3
11	Система защитных мер в психологическом информационном пространстве.	3

4.5 Самостоятельная работа

Семестр № 4

№	Вид СРС	Кол-во академических часов
1	Подготовка к зачёту	11
2	Подготовка к практическим занятиям	20
3	Проработка разделов теоретического материала	13

В ходе проведения занятий по дисциплине используются следующие интерактивные методы обучения: Дискуссия, кейс-технология,

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

Методические рекомендации к организации практическим занятиям представлены в методических указаниях: Информационно-психологическая безопасность в современном обществе: метод. указания по выполнению практических работы обучающихся / сост.: О.В. Пуляевская – Иркутск: Изд-во ИРНИТУ, 2021.

5.1.2 Методические указания для обучающихся по самостоятельной работе:

Задания представляют собой название темы, ее краткое содержание, основные понятия, вводимые в данной теме, контрольные вопросы и вопросы для обсуждения, источники с указанием страниц. Семинарские занятия предназначены для проверки у обучающегося уровня овладения объема содержания дисциплины. Во время занятий обучающемуся предоставляется возможность проверить, как идет формирование компетенций, насколько адекватны предъявляемым требованиям ответы обучающегося как в устной форме (по преимуществу), так и в письменной форме.
Каждый обучающийся на практическом занятии должен:

- участвовать в обсуждении темы практического занятия,
- показать, как идет усвоение понятий по теме,

• уметь отвечать и кратко (давая определения и приводя примеры), и развернуто, логически связывая различные разделы дисциплины,
• уметь работать в подгруппах, создавать сценарии, разрабатывать рекомендации.
В каждой теме перечислены все вопросы, понятия и их соотношения в том виде, в котором требует логика развертывания дисциплины. После разбора основных понятий следует обратить внимание на контрольные вопросы. Они сформулированы таким образом, что требуют краткого и точного ответа. Эти вопросы помогают обнаружить сложности в усвоении в теме. После проработки контрольных вопросов можно переходить к вопросам для обсуждения. Этот тип вопросов требует логического, последовательного рассуждения. Можно составлять по каждому такому вопросу небольшой план выступления-рассказа. В целом, формулировка такого вопроса совпадает с формулировкой вопросов для обсуждения по теме.

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 4 | Устный опрос

Описание процедуры.

к обсуждению к представлению ответов на следующие вопросы:
1.Дать сущностную характеристику понятию «информационное пространство».
2. Каковы особенности воздействия информационного пространства в современном обществе?
3. Что собой представляет характеристика культура кибербезопасности личности?
4. Какие есть методы социальной инженерии в информационно-психологическом пространстве в современном обществе?
5. Как осуществляется психологический анализ и оценка контента в системе OSINT?
6. Для чего используется профайлинг?
7. В чем заключаются особенности поведения людей в ситуации опасности?
8.Какие существуют факторы и причины угроз психологической безопасности человека?

Критерии оценивания.

способность демонстрировать знания теоретических идей и концепций в области информационно-психологической безопасности, умение аргументировать собственное мнение в процессе обсуждения вопросов с опорой на фундаментальные научные психологические факты.

6.1.2 семестр 4 | Творческое задание

Описание процедуры.

Работа в подгруппах (3-4 человека). Создать мультимедийный проект (эссе, презентацию, видеоролик или инфографику), в котором раскрыть определение кибервиктимности. Механизмы формирования виктимности. Анализ причин, по которым человек становится жертвой киберпреступлений. Влияние психологических аспектов (низкая самооценка, страх, агрессия). Требования к выполнению: использование креативных методов подачи информации; предложить реальные примеры или кейсы; максимально визуализировать данные (графики, схемы, инфографика). Обязательно обосновать выводы, подкрепить

сведениями из статей, научных исследований, статистики.

Критерии оценивания.

1. Глубина анализа и оригинальность подхода. 2. Качество визуальных и информационных материалов. 3. Логика и структурированность изложения. 4. Актуальность и практическая ценность предложенных решений. 5. Контакт с аудиторией. Каждый критерий оценивается по 5-бальной шкале.

6.1.3 семестр 4 | Собеседование

Описание процедуры.

Разделить обучающихся на подгруппы (2-4 человека). Каждая подгруппа будет выступать в роли интервьюеров и интервьюируемых. Нужно провести собеседование по подготовленной анкете, фокусируясь на выявлении угроз и стратегий защиты. Вопросы следующего плана: Какие личные данные вы обычно публикуете в сети? Бывали ли у вас ситуации кибербуллинга? Мошенничества? Какие действия вы предпринимаете при подозрении на угрозу? Что, по вашему мнению, помогает сохранять психологическую безопасность в сети? и т.д. Из полученных ответов составить краткое резюме, где отразить стратегии и механизмы, которые использует интервьюируемый, оценить осведомленность, предложить рекомендации.

Критерии оценивания.

Оценка анкеты для интервью: полнота и корректность вопросов для того, чтобы оценить стратегии и механизмы формирования психологической безопасности личности в киберпространстве - шкала 5 баллов. Оценка резюме: насколько удалось получить данные о стратегии и механизмах психологической безопасности личности в киберпространстве - шкала 5 баллов. Оценка предложенных рекомендаций, исходя из полученных данных - 5 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
ПКС-1.2	Способность проводить совместный анализ для выявления возможных источников информационных угроз, умение контролировать события безопасности, применять психологические средства и методы регуляции функциональных состояний в ситуации возможных информационно-психологических воздействий на личность и/или группу	Собеседование

6.2.2 Типовые оценочные средства промежуточной аттестации

6.2.2.1 Семестр 4, Типовые оценочные средства для проведения зачета по дисциплине

6.2.2.1.1 Описание процедуры

Зачет проводится в форме собеседования в процессе группового взаимодействия. Каждый участник предлагает развёрнуый вариант ответа на предложенные задачи/вопросы, участвует в дискуссии в процессе представления вариантов ответа других участников в процессе группового взаимодействия.

Пример задания:

Задача для собеседования: создать гипотетический сценарий использования шок-контента для социальной инженерии. Разработать рекомендации, как защититься от атак, использующих шок-контент. Фишинг-атака с шок-контентом: отправка сообщения с изображением или видео, вызывающим сильные эмоции (например, угроза безопасности или личной жизни), чтобы спровоцировать получателя на быстрые действия.
Запугивание через фейковые новости: создание сообщения о якобы произошедшем инциденте, требующем срочного реагирования или передачи данных.
Вымогательство: использование шокирующих изображений или информации для давления на жертву с целью получения денег или доступа.

6.2.2.1.2 Критерии оценивания

Зачтено	Не зачтено
Обучающийся демонстрирует способность проводить совместный анализ для выявления возможных источников информационных угроз, умение контролировать события безопасности, применять психологические средства и методы регуляции функциональных состояний в ситуации возможных информационно-психологических воздействий на личность и/или группу	Обучающийся не демонстрирует способность проводить совместный анализ для выявления возможных источников информационных угроз, умение контролировать события безопасности, применять психологические средства и методы регуляции функциональных состояний в ситуации возможных информационно-психологических воздействий на личность и/или группу

7 Основная учебная литература

1. Столяренко Л. Д. Основы психологии : учебное пособие для вузов / Л. Д. Столяренко, 2009. - 671.

2. Ларионова Л. А. Информационно-психологическая безопасность в современном обществе : электронный курс / Л. А. Ларионова, А. А. Маринов, 2023

8 Дополнительная учебная литература и справочная

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

2. Когнитивная психология : учеб. для вузов / [И. В. Блинникова, А. Н. Воронин, В. Н. Дружинин и др.], 2002. - 478.

3. Панкратов В. Н. Манипуляции в общении и их нейтрализация : практ. рук. / В. Н. Панкратов, 2001. - 201.

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

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. Microsoft Windows Seven Professional [1x100] RUS (проведен апгрейд с Microsoft Windows Seven Starter [1x100]) - поставка 2010

12 Материально-техническое обеспечение дисциплины

1. Интерактивная доска в комплекте (проектор,колонки,кабель)