Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 23.10.2023 17:19:58
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Декан факультета информационных технологий

/Д. Г. Демидов/

"30" августа 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Социально-психологические аспекты информационной безопасности»

Направление подготовки

10.05.03 «Информационная безопасность автоматизированных систем»

Образовательная программа (профиль)

«Безопасность открытых информационных систем»

Квалификация (степень) выпускника

Специалист по защите информации

Очная

Год приема - 2021

Москва 2021 г.

1. Цели освоения дисциплины.

К **основным целям** освоения дисциплины «Социально-психологические аспекты информационной безопасности» следует отнести:

- получение студентами специальных, как теоретических, так и практических знаний и компетенций в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, норм профессиональной этики, коммуникации, командной работы и лидерства;
- обеспечение понимания студентами информации, имеющей ключевое значение для принятия решений, формирование у них навыков критического мышления;
- закрепление получаемых в семестре знаний и навыков на практике;
- формирование взаимосвязей, получаемых в семестре знаний и навыков с изученными ранее;
- подготовка студентов к деятельности в соответствии с квалификационной характеристикой.

К **основным задачам** освоения дисциплины «Социально-психологические аспекты информационной безопасности» следует отнести:

- ознакомить студентов с общими теоретическими закономерностями в области коммуникации, психологии и социологии и значением этих закономерностей для обеспечения информационной безопасности;
- сформировать и развить способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи по информационной безопасности в части социально-психологических аспектов;
- сформировать и развить способность осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий;
- научить понимать социальную значимость своей будущей профессии, методы финансовой и нефинансовой мотивации к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдению норм профессиональной этики;
- научить выявлять современные угрозы информационной безопасности и их социально-психологические аспекты, определять фишинговые рассылки, приемы социально-психологического воздействия на человека;
- привить навыки работы в коллективе, толерантно воспринимая социальные, культурные и иные различия;
- сформировать навыки коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности.

2. Место дисциплины в структуре ООП.

Дисциплина «Социально-психологические аспекты информационной безопасности» относится к числу профессиональных учебных базовой части цикла (Б.1) основной образовательной программы (Б.1.22).

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Основы информационной безопасности», «Основы ИКТ», «Криптографические методы защиты информации», «Навыки эффективной презентации», «Сети и системы передачи данных».

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы.

В результате освоения дисциплины (модуля) у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код компетенции	**В результате освоения образовательной программы обучающийся должен обладать**	**Перечень планируемых результатов обучения по дисциплине**
ОПК—1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	**знать:** основные нормативные правовые акты в области информационной безопасности, профессиональную этику **уметь:** выступать с презентациями по вопросам профессиональной деятельности **владеть:** высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики
УК-3	Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	**Знать:** - эффективность использования стратегии сотрудничества для достижения поставленной цели, определяет свою роль в команде; - особенности поведения выделенных групп людей, с которыми работает/взаимодействует, учитывать их в своей деятельности; **Уметь:** моделировать ситуации, прогнозировать результаты (последствия) личных действий и планировать последовательность шагов для достижения заданного результата; **Владеть:** навыками эффективного взаимодействия с другими членами команды, в т.ч. навыками участия в обмене информацией, знаниями и опытом, и приемами эффективной презентации результатов работы команды.
УК-4	Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)	**Знать:** подходы к выбору на государственном и иностранном (-ых) языках коммуникативно приемлемых стилей делового общения, вербальных и невербальных средств взаимодействия с партнерами; **Уметь:** - использовать информационно- коммуникационные технологии при поиске необходимой информации в процессе решения стандартных коммуникативных задач на государственном и иностранном (- ых) языках; - вести деловую переписку, учитывая особенности стилистики официальных и неофициальных писем, социокультурные различия в формате корреспонденции на государственном и иностранном (-ых) языках;

		- использовать диалогическое общение для сотрудничества в академической коммуникации общения: • внимательно слушая и пытаясь понять суть идей других, даже если они противоречат собственным воззрениям; • уважая высказывания других как в плане содержания, так и в плане формы; • критикуя аргументированно и конструктивно, не задевая чувств других; • адаптируя речь и язык жестов к ситуациям взаимодействия. **Владеть:** навыками выполнять перевод профессиональных текстов с иностранного (-ых) на государственный язык и обратно.

4. Структура и содержание дисциплины.

Общая трудоемкость дисциплины составляет 2 зачетных единицы, т.е. **72** академических часов (лабораторные занятия – 36 час, самостоятельная работа - 36 часов, форма контроля – зачет) в 4 семестре.

Структура и содержание дисциплины «Социально-психологические аспекты информационной безопасности» по срокам и видам работы отражены в приложении.

Содержание разделов дисциплины

Вводный видеоурок

Предмет, цели и задачи курса «Социально-психологические аспекты информационной безопасности».

- Предмет, цели и задачи курса.
- Дорожная карта и результат курса.
- Концепция, этапы, содержание учебной работы.

Тема 1. Комплексный и междисциплинарный характер работы в области информационной безопасности. Влияние социально-психологических аспектов на обеспечение информационной безопасности.

(лабораторные работы – 6 часов, самостоятельная работа студентов – 6 часов)

Лабораторная работа 1.1. Комплексный и междисциплинарный характер работы в области информационной безопасности: социально-психологические аспекты

(2 часа)

- Основные тенденции в области информационной безопасности.
- Современные угрозы информационной безопасности и их социально-психологические аспекты, выявление фишинговых рассылок, приемов социально-психологического воздействия на человека.
- Комплексный и междисциплинарный характер работы в области информационной безопасности.
- Основные нормативные правовые акты в области информационной безопасности.

- Взаимосвязь информационной безопасности и непрерывности бизнеса.
- Социальная значимость профессии.
- Финансовая и нефинансовая мотивация к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства.
- Нормы профессиональной этики.

Лабораторная работа 1.2. Проекты в области информационной безопасности и социально-психологические аспекты их реализации.

(2 часа)

- Проектное управление: теоретические и методологические основы.
- Формулирование в рамках поставленной цели проекта совокупности взаимосвязанных задач, обеспечивающих ее достижение.
- Определение ожидаемые результаты решения выделенных задач.
- Проектирование решения конкретной задачи проекта, выбирая оптимальный способ ее решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений.
- Решение конкретных задач проекта заявленного качества и за установленное время.
- Публичное представление результатов решения конкретной задачи проекта.
- Социально-психологические аспекты подготовки и реализации проектов в области информационной безопасности.
- Выявление, анализ и решение проблемных вопросов.

Лабораторная работа 1.3. Социально-психологические аспекты проекта по внедрению системы менеджмента информационной безопасности в соответствии с ISO/IEC 27001:2013

- Практика формулирования в рамках поставленной цели проекта совокупности взаимосвязанных задач, обеспечивающих ее достижение.
- Практика определения ожидаемые результаты решения выделенных задач.
- Практика проектирования решения конкретной задачи проекта, выбирая оптимальный способ ее решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений.
- Практика решения конкретных задач проекта заявленного качества и за установленное время.
- Практика публичного представления результатов решения конкретной задачи проекта.
- Социально-психологические аспекты подготовки и реализации проектов, связанных с внедрением системы менеджмента информационной безопасности в соответствии с ISO/IEC 27001:2013.
- Социально-психологические аспекты проведения расследований в области информационной безопасности, поведенческого аудита.
- Выявление, анализ и решение проблемных вопросов.

Самостоятельная работа студентов (СРС)

(6 часов)

Видеоурок №1.

Резюме по теме 1.

Самостоятельное изучение студентами теоретических и практических вопросов. Изучение дополнительного теоретического материала, в том числе:

- Понятие социально-психологических аспектов информационной безопасности
- КОНТУР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЁРЧИНФОРМ: контроль всех потоков информации и предотвращение утечек. 2019
- Исследования и разработки по информационной безопасности и их опора на социальные и психологические данные. Предпосылки для нарушения информационной безопасности.

Тема 2. Командная работа и лидерство
(лабораторные работы – 10 часов, самостоятельная работа студентов – 10 часов)

Лабораторная работа 2.1. Работа в коллективе, в команде.
(2 часа)

- Личность. Сотрудник и коллектив. Команда проекта.
- Кадровые вопросы обеспечения информационной безопасности.
- Целеполагание компании, команды.
- Стратегия сотрудничества.
- Эффективное использование стратегии сотрудничества для достижения поставленной цели.
- Определение роли в команде.
- Особенности поведения выделенных групп людей.
- Эффективное взаимодействие с другими членами команды.
- Навыки участия в обмене информацией, знаниями и опытом.
- Приемы эффективной презентации результатов работы команды.
- Проблемы профессионального выгорания и способы их решения.
- Лидерство. Типы. Качества лидера.

Лабораторная работа 2.2. Команда центра реагирования на киберугрозы (SOC).
(2 часа)

- Требования к команде SOC: социально-психологические аспекты.
- Анализ практической ситуации: Solar JSOC – крупнейший центр защиты от киберугроз и провайдер сервисов информационной безопасности в России.
- Анализ практической ситуации: SOC компании.
- Проблемы кадрового обеспечения SOC.
- Анализ практической ситуации: анализ вакансий SOC, требований к кандидатам.
- Финансовая и нефинансовая мотивация команды SOC.
- Анализ практической ситуации: формирование кадрового резерва SOC.
- Руководитель SOC.

Лабораторная работа 2.3. Проектная группа внедрения системы менеджмента информационной безопасности в соответствии с ISO/IEC 27001:2013
(2 часа)

- Требования к команде внедрения: социально-психологические аспекты.
- Анализ практической ситуации: формирование проектной команды.
- Анализ практической ситуации: деятельность проектной команды.

- Проблемы кадрового обеспечения.
- Финансовая и нефинансовая мотивация команды.
- Формирование кадрового резерва при внедрении системы менеджмента информационной безопасности в соответствии с ISO/IEC 27001:2013.
- Лидерство при внедрении системы менеджмента информационной безопасности в соответствии с ISO/IEC 27001:2013.

Лабораторная работа 2.4. Команда аудиторов системы менеджмента информационной безопасности в соответствии с ISO/IEC 27001:2013

(2 часа)

- Требования к команде аудиторов: социально-психологические аспекты.
- Анализ практической ситуации: формирование команды внутренних аудиторов.
- Анализ практической ситуации: команда аудиторов при проведении сертификационного аудита.
- Анализ практической ситуации: команда аудиторов при проведении аудита поставщика.
- Проблемы кадрового обеспечения.
- Финансовая и нефинансовая мотивация команды.
- Формирование кадрового резерва внутренних аудиторов при внедрении системы менеджмента информационной безопасности в соответствии с ISO/IEC 27001:2013.
- Руководитель команды аудиторов.

Лабораторная работа 2.5. Команда аудиторов системы менеджмента непрерывности бизнеса в соответствии с ISO 22301:2019

(2 часа)

- Требования к команде аудиторов: социально-психологические аспекты.
- Анализ практической ситуации: формирование команды внутренних аудиторов.
- Анализ практической ситуации: команда аудиторов при проведении сертификационного аудита системы менеджмента непрерывности бизнеса в соответствии с ISO 22301:2019
- Анализ практической ситуации: команда аудиторов при проведении аудита поставщика с позиций непрерывности бизнеса.
- Проблемы кадрового обеспечения.
- Финансовая и нефинансовая мотивация команды.
- Формирование кадрового резерва внутренних аудиторов при внедрении системы менеджмента непрерывности бизнеса в соответствии с ISO 22301:2019.
- Лидерство при внедрении системы менеджмента непрерывности бизнеса в соответствии с ISO 22301:2019.
- Руководитель команды аудиторов.

Самостоятельная работа студентов (СРС)

(10 часов)

Видеоурок №2. Мотивы действия хакера

Резюме по теме 2.

Самостоятельное изучение студентами теоретических и практических вопросов.

Изучение дополнительного теоретического и практического материала, в том числе:

- The Hacker Report 2019
- The Hacker Report 2018
- ОБЗОР ОСНОВНЫХ ТИПОВ КОМПЬЮТЕРНЫХ АТАК В КРЕДИТНО-ФИНАНСОВОЙ СФЕРЕ в 2018 году
- «Web testing и атака на веб-приложение» по ссылке:https://cryptoworld.su/web-testing-i-ataka-na-veb-prilozhenie/

Работа с документами по теме курса в справочно-правовой системе «Консультант Плюс», «Гарант» и др. (по выбору студента)

Тема 3. Результаты личных действий. Планирование последовательности шагов для достижения заданного результата.

(лабораторные работы – 6 часов, самостоятельная работа студентов – 6 часов)

Лабораторная работа 3.1. Моделирование действий специалиста SOC

(2 часа)

- Моделирование ситуации.
- Прогнозирование результатов (последствий) личных действий и планирование последовательности шагов для достижения заданного результата.
- Практическая ситуация: моделирование действий специалиста SOC.

Лабораторная работа 3.2. Моделирование действий участника проектной группы внедрения системы менеджмента информационной безопасности в соответствии с ISO/IEC 27001:2013

(2 часа)

- Моделирование ситуации.
- Прогнозирование результатов (последствий) личных действий и планирование последовательности шагов для достижения заданного результата.
- Практическая ситуация: моделирование действий участника проектной группы внедрения системы менеджмента информационной безопасности в соответствии с ISO/IEC 27001:2013.

Лабораторная работа 3.3. Моделирование действий аудитора в области информационной безопасности

(2 часа)

- Моделирование ситуации.
- Прогнозирование результатов (последствий) личных действий и планирование последовательности шагов для достижения заданного результата.
- Практическая ситуация: моделирование действий внутреннего аудитора системы менеджмента информационной безопасности в соответствии с ISO/IEC 27001:2013.
- Практическая ситуация: моделирование действий аудитора системы менеджмента информационной безопасности в соответствии с ISO/IEC 27001:2013 при проведении сертификационного аудита.
- Практическая ситуация: моделирование действий аудитора системы менеджмента непрерывности бизнеса в соответствии с ISO 22301:2019 при проведении сертификационного аудита.
- Практическая ситуация: моделирование действий аудитора поставщика

Самостоятельная работа студентов (СРС)

(6 часов)

Самостоятельное изучение студентами теоретических и практических вопросов.

Изучение дополнительного теоретического и практического материала.

Анализ практических ситуаций

Анализ форм и методов обучения (в форме лекций, обучающих презентаций, обучающих видеороликов, плакатов и иных наглядных материалов, игрофикация обучения), тестирования, повторного тестирования, личных бесед;

Изучение подходов к составлению программы обучения работников предприятия по вопросам социально-психологических аспектов информационной безопасности применительно к актуальным вопросам социальной инженерии.

Тема 4. Коммуникации и критическое мышление.

(лабораторные работы – 8 часов, самостоятельная работа студентов – 8 часов)

Лабораторная работа 4.1. Коммуникации. Критическое мышление и когнитивная гибкость как необходимые навыки.

(2 часа)

- Коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности.
- Подходы к выбору на государственном и иностранном (-ых) языках коммуникативно приемлемых стилей делового общения, вербальных и невербальных средств взаимодействия с партнерами.

Лабораторная работа 4.2. Поиск информации. Ведение деловой переписки.

(2 часа)

- Использование информационно-коммуникационные технологии при поиске необходимой информации в процессе решения стандартных коммуникативных задач на государственном и иностранном (- ых) языках.
- Ведение деловой переписки, учитывая особенности стилистики официальных и неофициальных писем, социокультурные различия в формате корреспонденции на государственном и иностранном (-ых) языках.
- Значение двух неразрывных принципов: (1) умение быстро ориентироваться в стремительно растущем потоке информации и находить нужное, и (2) умение осмыслить и применить полученную информацию.
- Навыки и умения, которые будут востребованы и актуальны в самом ближайшем будущем: комплексное решение проблем (Complex problem solving), критическое мышление (Critical thinking), креативность (Creativity), управление людьми (People management), взаимодействие с людьми (Coordinating with others), коммуникация, эмоциональный интеллект (Emotional intelligence), формирование собственного мнения и принятие решений (Judgment and decision-making) и когнитивная гибкость (Cognitive flexibility).
- Понятие «критическое мышление». Обучение элементам критического мышления при поиске информации и ведении деловой переписки.
- Эффективная работа с информацией.

Лабораторная работа 4.3. Диалогическое общение.

(2 часа)

- Использование диалогического общения для сотрудничества в академической коммуникации общения:
  - внимательно слушая и пытаясь понять суть идей других, даже если они противоречат собственным воззрениям;
  - уважая высказывания других как в плане содержания, так и в плане формы;
  - критикуя аргументированно и конструктивно, не задевая чувств других;
  - адаптируя речь и язык жестов к ситуациям взаимодействия.
- Кейсы (практические ситуации).
- Выполнение перевода профессиональных текстов с иностранного (-ых) на государственный язык и обратно.
- Работа с оригинальными текстами, документами и материалами по информационной безопасности на русском и английском языках.

Лабораторная работа 4.4. Критический инструментарий для принятия решений. Типы манипуляций и методы защиты от них.

(2 часа)

- Критический инструментарий для принятия решений.
- Эффективная работа с информацией. Логика. Логика интерпретаций. Вопросы. Тактика убеждения. Правильная аргументация и доказательство. Основные приемы опровержения и критика.
- Критический инструментарий для принятия решений. Технологии принятия решений. Решение задач. Проектирование стратегии.
- Анализ целей и типов манипуляций.
- Анализ методов защиты от манипуляций.
- Кейсы (практические ситуации).
- Выполнение перевода профессиональных текстов с иностранного (-ых) на государственный язык и обратно.
- Работа с оригинальными текстами, документами и материалами по информационной безопасности на русском и английском языках.

Самостоятельная работа студентов (СРС)

(8 часов)

Самостоятельное изучение студентами теоретических и практических вопросов.

Изучение дополнительного теоретического и практического материала, в том числе

- Винсент Руджеро "По ту сторону эмоций и чувств. Руководство по критическому мышлению" https://gtmarket.ru/laboratory/basis/4466
- Питер Фасиоун "Критическое мышление: что это такое и почему это важно?" http://www.evolkov.net/critic.think/Facione_P/Crit_Think_What_It_Is_and_Why_It_Counts.Facione.P.html
- Ричард Поль «Критическое мышление: что необходимо каждому для выживания в быстро меняющемся мире»
- http://www.evolkov.net/critic.think/Paul.R/Paul.R.Critical.thinking.21.html
- Максим Власов «Психология принятия решений» https://psichel.ru/psihologiya-prinyatiya-reshenij/
- Джорджио Нардонэ «Страх принятия решений» https://www.b17.ru/article/77260/
- Чип Хиз и Дэн Хиз «Ловушки мышления»http://www.rulit.me/books/lovushki-myshleniya-kak-prinimat-resheniya-o-kotoryh-vy-ne-pozhaleete-read-335897-24.html

- «Системы поддержки принятия решений» http://www.tstu.ru/book/elib3/mm/2017/maistrenko/t6.html
- Неряхин Н. Я манипулирую тобой: Методы противодействия скрытому влиянию /Никита непряхин. – М.: Альпина Паблишер, 2019.
- «Десять хитрых тактик манипуляторов» https://4brain.ru/blog/хитрые-тактики-манипуляторов/
- «7 простых и 7 сложных приемов манипуляции сознанием. Какие из них используют на вас?» http://www.aif.ru/money/business/29151
- «Приемы манипуляции в дискуссии» https://4brain.ru/blog/приемы-манипуляции-в-дискуссии/
- Описание и назначение тестов по ссылке:
- https://www.cognifit.com/ru/science/cognitive-skills
- Тест для самопроверки по ссылке: https://digitaltests.ru/
- Тест для самопроверки по ссылке: http://critical-thinking.ru/test/
- Тест для самопроверки по ссылке: https://evolkov.net/critic.think/tests/

Тема 5. Социально-психологические технологии, позволяющие обезопасить физических и юридических лиц (компании, банки) от воздействия хакеров в ежедневном взаимодействии в сети

(лабораторные работы – 6 часов, самостоятельная работа студентов – 6 часов)

Лабораторная работа 5.1. Встраивание систем защиты от воздействия хакеров (социально-психологические аспекты)

(2 часа)

- Социально-психологические технологии, позволяющие обезопасить физических и юридических лиц (компании, банки) от воздействия хакеров в ежедневном взаимодействии в сети.
- Встраивание систем защиты от воздействия хакеров (социально-психологические аспекты) в информационную безопасность организации. Меры организационного характера. Система разграничения доступа к информации. Локальные нормативные акты организации. Разъяснения и рекомендации. Роль сотрудников организации. Обучение сотрудников по вопросам информационной безопасности.
- Расследования в области информационной безопасности, поведенческий аудит.
- Кейсы (практические ситуации).
- Выполнение перевода профессиональных текстов с иностранного (-ых) на государственный язык и обратно.
- Работа с оригинальными текстами, документами и материалами по информационной безопасности на русском и английском языках.

Лабораторная работа 5.2. Социально-психологические аспекты совершенствования управления информационной безопасностью.

(2 часа)

- Социально-психологические аспекты совершенствования управления информационной безопасностью организации.
- Кейсы (практические ситуации).
- Выполнение перевода профессиональных текстов с иностранного (-ых) на государственный язык и обратно.
- Работа с оригинальными текстами, документами и материалами по информационной безопасности на русском и английском языках.

Лабораторная работа 5.3. Изучение и анализ практических материалов по информационной безопасности ФСТЭК, Интерпола, Европола

(2 часа)

- Кейсы (практические ситуации).
- Выполнение перевода профессиональных текстов с иностранного (-ых) на государственный язык и обратно.
- Работа с оригинальными текстами, документами и материалами по информационной безопасности на русском и английском языках.

Самостоятельная работа студентов (СРС)

(6 часов)

Самостоятельное изучение студентами теоретических и практических вопросов.

- Изучение дополнительного теоретического материала.
- Работа с Банком данных угроз безопасности информации и ознакомление с Проектом методического документа «Методика моделирования угроз безопасности информации»
    - Банк данных угроз безопасности информации (доступно по ссылке: https://bdu.fstec.ru/);

  информация применительно к угрозам информационной безопасности, Информационное сообщение о разработке методического документа ФСТЭК России «Методика определения угроз безопасности информации в информационных системах» от 9 апреля 2020 г. № 240/22/1534
  https://fstec.ru/component/attachments/download/2728
  https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy
    - Проект методического документа «Методика моделирования угроз безопасности информации»

  https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/149-proekty/2070-metodicheskij-dokument
    - Методический документ должен применяться совместно с банком данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru)
    - Видео-обзор (7-8 минут) новой методики моделирования угроз безопасности информации от ФСТЭК России.

  https://www.youtube.com/watch?v=yW36ASIkDFE&fbclid=IwAR31WI1UT4UsdV3pbtt3mrk2maXdfOwyWTSif1fOn8_UX025WTnYUi_WzEM
- Ознакомление со статьей «Платформа автоматизированного реагирования на инциденты ИБ»

https://habr.com/ru/company/technoserv/blog/491384/

5. Образовательные технологии.

Методика преподавания дисциплины «Социально-психологические аспекты информационной безопасности» и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся:

- подготовка к выполнению лабораторных работ;

Удельный вес занятий, проводимых в интерактивных формах по дисциплине, составляет 100% аудиторных занятий.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов.

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- компьютерное тестирование;
- зачет.

Образцы тестовых заданий, билетов для зачета, приведены в приложении.

6.1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю).

6.1.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.
В результате освоения дисциплины (модуля) формируются следующие компетенции:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать
ОПК—1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства
УК-3	Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде
УК-4	Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются поэтапно в ходе освоения обучающимися дисциплин (модулей), практик в соответствии с учебным планом и календарным графиком учебного процесса.

6.1.2. Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины (модуля), описание шкал оценивания

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине (модулю).
Шкалы оценивания результатов промежуточной аттестации и их описание.

Форма промежуточной аттестации: зачет.

Промежуточная аттестация обучающихся в форме зачета проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется: «зачтено» или «не зачтено».

Шкала оценивания	**Описание**
Зачтено	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Не зачтено	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

Фонды оценочных средств представлены в приложении к рабочей программе.

7. Учебно-методическое и информационное обеспечение дисциплины.

а) Основная литература:

1. Кибербезопасность цифровой индустрии. Теория и практика устойчивости к кибератакам / Под редакцией профессора РАН, доктора технических наук Д.П. Зегжды. – М.: Горячая линия – Телеком, 2020. – 560 с.: ил.
2. Лидерство /Пер. с англ. – 3-е изд. – М. : Альпина Паблишер, 2020 (Серия «Harvard Business Review 10 лучших статей»).
3. Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление инцидентами информационной безопасности и непрерывностью бизнеса. Учебное пособие для вузов. - 2-е изд., испр. - М.: Горячая линия - Телеком, 2019. - 170 с.: ил. - Серия "Вопросы управления информационной безопасностью. Выпуск 3".
4. Эффективные коммуникации / Пер. с англ. – М. : Альпина Паблишер, 2020. – 200 с. – (Серия «Harvard Business Reviev: 10 лучших статей).
5. Чатфилд Т. Критическое мышление: Анализируй, сомневайся, формируй свое мнение / Том Чатфилд; Пер. с англ. – М.: Альбина Паблишер, 2019. – 328 с., ил.

Перечень основных нормативных документов

1. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями).

2. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных» (с изменениями и дополнениями).
3. Федеральный закон от 26 июля 2006 г. N 135-ФЗ «О защите конкуренции» (с изменениями и дополнениями).
4. Федеральный закон от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (с изменениями и дополнениями)
5. Федеральный закон от 29.07.2004 N 98-ФЗ «О коммерческой тайне» (с изменениями и дополнениями).
6. Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

Международные стандарты

1. ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements.
2. ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements.

б) дополнительная литература:

1. Гилязова Р. Н. Информационная безопасность. Лабораторный практикум. Учебное пособие. Издательство Лань. Санкт-Петербург, 2020. - 44 с. (доступно по ссылке: https://e.lanbook.com/reader/book/130179/#22)
2. Гродзенский Я. С. Информационная безопасность. Издательство: ПРОСПЕКТ : РГ-Пресс. Москва, 2020.
3. Кови С.Р. Семь навыков высокоэффективных людей: мощные инструменты развития личности /Ставен Р.Кови ; пер. с англ. – 13-е изд., доп. – М. : Альпина Паблишер, 2019.
4. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С.М. Корабельников. – Москва : Издательство Юрайт, 2020. – 111 с. – (Высшее образование).
5. Чернова Е.В. Информационная безопасность человека. Учебное пособие для вузов. Издательство Юрайт. Москва, 2020. – 243 с.
6. Kali Linux. Тестирование на проникновение и безопасность. – Питер, 2020.

в) программное обеспечение и интернет-ресурсы:

Программное обеспечение: Word, Excel, PowerPoint, программное обеспечение для просмотра видео- и аудиоконтента и др.

Интернет-ресурсы:

- Банк данных угроз безопасности информации (доступно по ссылке: https://bdu.fstec.ru/);

- Информационное сообщение о разработке методического документа ФСТЭК России «Методика определения угроз безопасности информации в информационных системах» от 9 апреля 2020 г. № 240/22/1534

https://fstec.ru/component/attachments/download/2728

https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy

- Проект методического документа «Методика моделирования угроз безопасности информации»

https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/149-proekty/2070-metodicheskij-dokument

Методический документ должен применяться совместно с банком данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru)

- Видео-обзор (7-8 минут) новой методики моделирования угроз безопасности информации от ФСТЭК России.

https://www.youtube.com/watch?v=yW36ASIkDFE&fbclid=IwAR31WI1UT4UsdV3pbtt3mrk2maXdfOwyWTSif1fOn8_UX025WTnYUi_WzEM

- Имре Лакатос «Доказательства и опровержения» https://gtmarket.ru/laboratory/basis/4382/4387

- «Как правильно критиковать. Практическое руководство» https://www.factroom.ru/obshchestvo/how-to-criticize-constructively

- Пири Мэдсен «Железные аргументы» https://psy.wikireading.ru/16472

- «Способы ухода от ответа на вопрос» https:// https://4brain.ru/blog/способы-ухода-от-ответа-на-вопрос/

- «Гибкая реакция на жесткие вопросы» https:// https://4brain.ru/blog/чёрная-риторика-4/

- «Как отвечать на неудобные вопросы?» https:// https://4brain.ru/blog/ответы-на-неудобные-вопросы/

- «Объясняем основные принципы социальной инженерии» (автор Денис Матвеев) в сети Интернет по ссылке:

- Шермер Майкл "Скептик: Рациональный взгляд на мир" https://avidreaders.ru/read-book/skeptik-racionalnyy-vzglyad-na-mir.html

- Винсент Руджеро "По ту сторону эмоций и чувств. Руководство по критическому мышлению" https://gtmarket.ru/laboratory/basis/4466

- Питер Фасиоун "Критическое мышление: что это такое и почему это важно?" http://www.evolkov.net/critic.think/Facione_P/Crit_Think_What_It_Is_and_Why_It_Counts.Facione.P.html

- Ричард Поль «Критическое мышление: что необходимо каждому для выживания в быстро меняющемся мире»

http://www.evolkov.net/critic.think/Paul.R/Paul.R.Critical.thinking.21.html

- Максим Власов «Психология принятия решений» https://psichel.ru/psihologiya-prinyatiya-reshenij/

- Джорджио Нардонэ «Страх принятия решений» https://www.b17.ru/article/77260/

- Чип Хиз и Дэн Хиз «Ловушки мышления» http://www.rulit.me/books/lovushki-myshleniya-kak-prinimat-resheniya-o-kotoryh-vy-ne-pozhaleete-read-335897-24.html

- «Системы поддержки принятия решений» http://www.tstu.ru/book/elib3/mm/2017/maistrenko/t6.html

- «Web testing и атака на веб-приложение» по ссылке:https://cryptoworld.su/web-testing-i-ataka-na-veb-prilozhenie/

- «Десять хитрых тактик манипуляторов» https://4brain.ru/blog/хитрые-тактики-манипуляторов/

- «7 простых и 7 сложных приемов манипуляции сознанием. Какие из них используют на вас?» http://www.aif.ru/money/business/29151

- «Приемы манипуляции в дискуссии» https://4brain.ru/blog/приемы-манипуляции-в-дискуссии/

- Описание и назначение тестов по ссылке:

https://www.cognifit.com/ru/science/cognitive-skills

8. Материально-техническое обеспечение дисциплины.

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, экран) – 1 комплект.

1. Операционная система Windows 7 или более поздней версии или аналог.

2. Microsoft Office XP или более поздней версии или аналог.
3. Антивирусное ПО «Kaspersky Antivirus» 7.0 или более поздней версии или аналог.

Для проведения лабораторных занятий необходимо наличие компьютерных классов, оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

Система LMS.

Оборудование и аппаратура.

1 презентационное оборудование (мультимедийный проектор, экран) – 1 комплект.

Персональный компьютер (из расчета 1 оборудованное рабочее место на одного обучаемого).

Компьютерный класс с доступом к сети Интернет.

1. Веб-браузер Chrome.
2. Microsoft Visual Studio.
3. Microsoft Office.

9. Методические рекомендации для самостоятельной работы студентов

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются лабораторные работы и самостоятельная работа студентов.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, готовятся к зачету, а также самостоятельно изучают отдельные темы учебной программы.

10. Методические рекомендации для преподавателя

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки **10.05.03 «Информационная безопасность автоматизированных систем»**.

Программу составил: доц. Темникова К.Н., к.э.н.

Программа утверждена на заседании кафедры “Информационная безопасность” «30» августа 2021 г., протокол № 1

Заведующий кафедрой
«Информационная безопасность»



к.т.н., доцент Н.В. Федоров

Приложение.

**Структура и содержание дисциплины «Социально-психологические аспекты информационной безопасности»
по направлению подготовки
10.05.03 «Информационная безопасность автоматизированных систем»
(специалист)**

n/n	Раздел	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов, и трудоемкость в часах					Виды самостоятельной работы студентов					Формы аттестации	
				Л	П/С	Лаб	СРС	КСР	К.Р.	К.П.	ДЗ	Реферат	К/р	Э	З
	4 семестр														
1	Вводный видеоурок **Тема 1.** Комплексный и междисциплинарный характер работы в области информационной безопасности. Влияние социально-психологических аспектов на обеспечение информационной безопасности. ***Лабораторная работа 1.1.*** Комплексный и междисциплинарный характер работы в области информационной безопасности: социально-психологические аспекты	4	1			2	2								
2	***Лабораторная работа 1.2.*** Проекты в области информационной безопасности и социально-		2			2	2								

	психологические аспекты их реализации.															
3	***Лабораторная работа 1.3.*** Социально-психологические аспекты проекта по внедрению системы менеджмента информационной безопасности в соответствии с ISO/IEC 27001:2013		3			2	2								
4	**Тема 2. Командная работа и лидерство** ***Лабораторная работа 2.1.*** Работа в коллективе, в команде.		4			2	2								
5	***Лабораторная работа 2.2.*** Команда центра реагирования на киберугрозы (SOC).		5			2	2								
6	***Лабораторная работа 2.3.*** Проектная группа внедрения системы менеджмента информационной безопасности в соответствии с ISO/IEC 27001:2013		6			2	2								
7	***Лабораторная работа 2.4.*** Команда аудиторов системы менеджмента информационной безопасности в соответствии с ISO/IEC 27001:2013.		7			2	2								
8	***Лабораторная работа 2.5.*** Команда аудиторов системы менеджмента непрерывности бизнеса в соответствии с ISO 22301:2019		8			2	2								
9	**Тема 3.** Результаты личных действий. Планирование последовательности шагов для достижения заданного результата.		9			2	2								

	Лабораторная работа 3.1. Моделирование действий специалиста SOC															
10	***Лабораторная работа 3.2.*** Моделирование действий участника проектной группы внедрения системы менеджмента информационной безопасности в соответствии с ISO/IEC 27001:2013		10			2	2									
	Лабораторная работа 3.3. Моделирование действий аудитора в области информационной безопасности		11			2	2									
	Тема 4. Коммуникации и критическое мышление. ***Лабораторная работа 4.1.*** Коммуникации. Критическое мышление и когнитивная гибкость как необходимые навыки.		12			2	2									
	Лабораторная работа 4.2. Поиск информации. Ведение деловой переписки.		13			2	2									
	Лабораторная работа 4.3. Диалогическое общение.		14			2	2									
	Лабораторная работа 4.4. Критический инструментарий для принятия решений. Типы манипуляций и методы защиты от них.		15			2	2									
	Тема 5. Социально-психологические технологии, позволяющие обезопасить физических и		16			2	2									

	юридических лиц (компании, банки) от воздействия хакеров в ежедневном взаимодействии в сети ***Лабораторная работа 5.1.*** Встраивание систем защиты от воздействия хакеров (социально-психологические аспекты)														
	Лабораторная работа 5.2. Социально-психологические аспекты совершенствования управления информационной безопасностью.		17			2	2								
	Лабораторная работа 5.3. Изучение и анализ практических материалов по информационной безопасности ФСТЭК, Интерпола, Европола		18			2	2								
	Форма аттестации	4	19-21							.				З	
	Всего часов по дисциплине во третьем семестре					36	36								
	Всего часов по дисциплине					36	36								

Приложение к
рабочей программе

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗРВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Направление подготовки: 10.05.03 «Информационная безопасность автоматизированных систем»

ОП (профиль): «Безопасность открытых информационных систем»

Форма обучения: очная

Вид профессиональной деятельности: эксплуатационная; проектно-технологическая; экспериментально-исследовательская; организационно-управленческая

Кафедра: «Информационная безопасность»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ

«Социально-психологические аспекты информационной безопасности»

Состав: 1. Паспорт фонда оценочных средств

2. Описание оценочных средств:

Компьютерное тестирование

Зачет

Составители: доц. Темникова К.Н.

Москва, 2021 год

Таблица 1

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Социально-психологические аспекты информационной безопасности					
ФГОС ВО **10.05.03 «Информационная безопасность автоматизированных систем»**					
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие **общепрофессиональные и профессиональные компетенции**:					
КОМПЕТЕНЦИИ		**Перечень компонентов**	**Технология формирования компетен**	**Форма оценоч-ного**	**Степени уровней освоения компетенций**
ИН-ДЕКС	**ФОРМУЛИРОВКА**				

ОПК—1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	**знать:** основные нормативные правовые акты в области информационной безопасности, профессиональную этику **уметь:** выступать с презентациями по вопросам профессиональной деятельности **владеть:** высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	самостоятельная работа, лабораторные занятия	КТ, Зачет	Базовый уровень: **знать:** основные нормативные правовые акты в области информационной безопасности, профессиональную этику **уметь:** выступать с презентациями по вопросам профессиональной деятельности **владеть:** высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики Повышенный уровень: **знать:** основные нормативные правовые акты в области информационной безопасности, профессиональную этику, лучшие практики деловых коммуникаций **уметь:** выступать с презентациями по вопросам профессиональной деятельности, в том числе при внедрении систем менеджмента информационной безопасности, системы менеджмента непрерывности деятельности **владеть:** навыками формирования системы финансовой и нефинансовой мотивации к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики

УК-3	Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	**Знать:** - эффективность использования стратегии сотрудничества для достижения поставленной цели, определяет свою роль в команде; - особенности поведения выделенных групп людей, с которыми работает/взаимодействует, учитывать их в своей деятельности; **Уметь:** моделировать ситуации, прогнозировать результаты (последствия) личных действий и планировать последовательность шагов для достижения заданного результата; **Владеть:** навыками эффективного взаимодействия с другими членами команды, в т.ч. навыками участия в обмене информацией, знаниями и опытом, и приемами эффективной презентации результатов работы команды.	самостоятельная работа, лабораторные занятия	КТ, Зачет	Базовый уровень: **Знать:** - эффективность использования стратегии сотрудничества для достижения поставленной цели, определяет свою роль в команде; - особенности поведения выделенных групп людей, с которыми работает/взаимодействует, учитывать их в своей деятельности; **Уметь:** моделировать ситуации, прогнозировать результаты (последствия) личных действий и планировать последовательность шагов для достижения заданного результата; **Владеть:** навыками эффективного взаимодействия с другими членами команды, в т.ч. навыками участия в обмене информацией, знаниями и опытом, и приемами эффективной презентации результатов работы команды. Повышенный уровень: **Знать:** - эффективность использования стратегии сотрудничества для достижения поставленной цели, определяет свою роль в команде; - особенности поведения выделенных групп людей, с которыми работает/взаимодействует, учитывать их в своей деятельности; **Уметь:** моделировать ситуации, прогнозировать результаты (последствия) личных действий и планировать последовательность шагов для достижения заданного результата при внедрении систем менеджмента информационной безопасности, системы менеджмента непрерывности деятельности **Владеть:** навыками эффективного взаимодействия с другими членами команды, в т.ч. навыками участия в обмене информацией, знаниями и опытом, и приемами эффективной презентации результатов работы команды

УК-4	Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)	**Знать:** подходы к выбору на государственном и иностранном (-ых) языках коммуникативно приемлемых стилей делового общения, вербальных и невербальных средств взаимодействия с партнерами; **Уметь:** - использовать информационно- коммуникационные технологии при поиске необходимой информации в процессе решения стандартных коммуникативных задач на государственном и иностранном (- ых) языках; - вести деловую переписку, учитывая особенности стилистики официальных и неофициальных писем, социокультурные различия в формате корреспонденции на государственном и иностранном (-ых) языках; - использовать диалогическое общение для сотрудничества в академической коммуникации общения: • внимательно слушая и пытаясь понять суть идей других, даже если они противоречат собственным воззрениям; • уважая высказывания других как в плане содержания, так и в плане формы; • критикуя аргументированно и конструктивно, не задевая чувств других; • адаптируя речь и язык жестов к ситуациям взаимодействия. **Владеть:** навыками выполнять перевод профессиональных текстов с иностранного (-ых) на государственный язык и обратно.			Базовый уровень: **Знать:** подходы к выбору на государственном и иностранном (-ых) языках коммуникативно приемлемых стилей делового общения, вербальных и невербальных средств взаимодействия с партнерами; **Уметь:** - использовать информационно-коммуникационные технологии при поиске необходимой информации в процессе решения стандартных коммуникативных задач на государственном и иностранном (- ых) языках; - вести деловую переписку, учитывая особенности стилистики официальных и неофициальных писем, социокультурные различия в формате корреспонденции на государственном и иностранном (-ых) языках; - использовать диалогическое общение для сотрудничества в академической коммуникации общения: **Владеть:** навыками выполнять перевод профессиональных текстов с иностранного (-ых) на государственный язык и обратно. Повышенный уровень: **Знать:** подходы к выбору на государственном и иностранном (-ых) языках коммуникативно приемлемых стилей делового общения, вербальных и невербальных средств взаимодействия с партнерами; **Уметь:** - использовать информационно- коммуникационные технологии при поиске необходимой информации в процессе решения стандартных коммуникативных задач на государственном и иностранном (- ых) языках; - вести деловую переписку, учитывая особенности стилистики официальных и неофициальных писем, социокультурные различия в формате корреспонденции на государственном и иностранном (-ых) языках; - использовать диалогическое общение для сотрудничества в академической коммуникации общения: • внимательно слушая и пытаясь понять суть идей других, даже если они противоречат собственным воззрениям; • уважая высказывания других как в плане

Приложение 2
к рабочей программе

Оценочные средства для текущей аттестации

Промежуточное тестирование

По каждой теме предлагается 25 вопросов для тестирования в системе LMS. Освоение темы зависит от результата написания теста: 23-25 баллов – тема считается освоенной на продвинутом уровне; 14-22 балла – тема считается освоенной на базовом уровне; 0-13 баллов – тема считается не освоенной. В тесте представлены задания/вопросы разных типов. Тест содержит вопросы по материалам теории и пройденных лабораторных работ.

Итоговое тестирование

Итоговый тест включает 70% промежуточных тестов, сформированных на основе случайного выбора из всего банка тестовых заданий/вопросов для промежуточного тестирования и 30% тестовых заданий/вопросов, отличных от промежуточных, то есть не вошедших в промежуточные тесты заданий/вопросов.

Тесты представлены в системе LMS.

Оценочные средства для промежуточной аттестации

Зачет

Зачет принимается либо в виде итогового теста в системе LMS, либо в устной форме при ответе на вопросы билета. В билете содержится 2 (два) вопроса.

Список вопросов для зачета по дисциплине

Вопросы к зачету

по курсу «Социально-психологические аспекты информационной безопасности»

1. Проекты в области информационной безопасности и социально-психологические аспекты их реализации.
2. Социально-психологические аспекты проекта по внедрению системы менеджмента информационной безопасности в соответствии с ISO/IEC 27001:2013.
3. Нормы профессиональной этики в области информационной безопасности.
4. Эффективность использования стратегии сотрудничества для достижения поставленной цели в области информационной безопасности.
5. Командная работа. Определение роли в команде.
6. Лидерство. Типы лидерства. Лидерство при внедрении системы менеджмента информационной безопасности в соответствии с ISO/IEC 27001:2013.
7. Социально-психологические аспекты проведения расследований в области информационной безопасности, поведенческого аудита.
8. Команда центра реагирования на киберугрозы (SOC). Требования к команде SOC: социально-психологические аспекты.
9. Проектная группа внедрения системы менеджмента информационной безопасности в соответствии с ISO/IEC 27001:2013. Требования к команде: социально-психологические аспекты.

10. Команда аудиторов системы менеджмента информационной безопасности в соответствии с ISO/IEC 27001:2013. Требования к команде аудиторов: социально-психологические аспекты.
11. Команда аудиторов системы менеджмента непрерывности бизнеса в соответствии с ISO 22301:2019. Требования к команде аудиторов: социально-психологические аспекты.
12. Результаты личных действий в области информационной безопасности. Планирование последовательности шагов для достижения заданного результата. Моделирование действий.
13. Моделирование действий внутреннего аудитора системы менеджмента информационной безопасности в соответствии с ISO/IEC 27001:2013.
14. Моделирование действий аудитора поставщика с позиции информационной безопасности.
15. Использование информационно-коммуникационные технологии при поиске необходимой информации в области информационной безопасности в процессе решения стандартных коммуникативных задач на государственном и иностранном (- ых) языках.
16. Коммуникации в области информационной безопасности в устной форме.
17. Коммуникации в области информационной безопасности в письменной форме.
18. Социально-психологические технологии, позволяющие обезопасить физических и юридических лиц (компании, банки) от воздействия хакеров в ежедневном взаимодействии в сети.
19. Социально-психологические аспекты расследований в области информационной безопасности, поведенческий аудит.
20. Социально-психологические аспекты обучения сотрудников компании по вопросам информационной безопасности.

Пример билета.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Курс «Социально-психологические аспекты информационной безопасности»

Зачет

Билет №__

Вопросы:

1. Проекты в области информационной безопасности и социально-психологические аспекты их реализации.
2. Команда внутренних аудиторов системы менеджмента информационной безопасности в соответствии с ISO/IEC 27001:2013. Требования к команде внутренних аудиторов: социально-психологические аспекты.