МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«МИРЭА – Российский технологический университет»

РТУ МИРЭА

Институт кибербезопасности и цифровых технологий (ИКБ)

КБ-2 «Информационно-аналитические системы кибербезопасности»

ОТЧЕТ О ВЫПОЛНЕНИИ ИНДИВИДУАЛЬНОГО ЗАДАНИЯ №1

В РАМКАХ ДИСЦИПЛИНЫ «ОСНОВЫ НАУЧНЫХ ИССЛЕДОВАНИЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Выполнил:

Студент 4-ого курса

Учебной группы БИСО-02-22

Зубарев В.С.

Москва 2025

Тема: Общие сведения о науке и научных исследованиях

Цель: Получение обучающимся общих сведений о науке и научных исследованиях.

Задание 1. Вставьте пропущенное слово

1. **Наука -** система знаний о природе, обществе, мышлении, об объективных законах их развития.

2. **Наука** - непрерывно развивающаясясистема знаний объективных законов природы, общества и мышления, которая сохраняется и развивается усилиями ученых.

3. **Познание -** творческая деятельность субъекта, ориентированная на получение достоверных знаний о мире.

4. **Знание -** проверенный практикой результат познания действительности, адекватное ее отображение в сознании человека.

5. Культурно-мировоззренческая функция: наука дает человеку знания об окружающем мире, помогает систематизировать их и формирует **мировоззрение** как составную часть **культуры**.

6. Представитель науки, осуществляющий осмысленную деятельность по формированию научной картины мира, чья научная деятельность и квалификация в той или иной форме получили признание со стороны научного сообщества – это **ученый**.

7. Наука дает человеку знания об окружающем мире, помогает систематизировать их и формирует **мировоззрение** составную часть **культуры**.

Задание 2. Объяснить основные понятия науки:

Методические основы науки; познавательные приёмы (как сравнение, измерение, индукция, дедукция, анализ, синтез); гипотеза, концепция, соотношение, объект исследования, предмет исследования, методику исследования.

Научная деятельность — это процесс систематического изучения мира, включающий формулирование гипотез, проведение экспериментов, сбор и анализ данных, а также разработку теорий. Цель научной деятельности — получение новых знаний и решение практических проблем.

Научная разработка — это процесс создания и внедрения новых знаний, технологий или методов на основе научных исследований. Она включает в себя разработку инновационных решений, приложений и технологий, основанных на теоретических и экспериментальных данных.

Эмпирические основы науки — это совокупность данных и фактов, полученных в результате наблюдений, экспериментов или опытов, которые служат основой для формирования научных теорий и гипотез. Эмпирические данные являются источником для проверки и подтверждения научных идей, обеспечивая объективность и достоверность научных выводов.

Методические основы науки — это система принципов, методов и подходов, которые формируют основу научного исследования и практики. Они включают в себя общие и специфические методы исследования, а также критерии, нормы и правила, которым должно следовать исследование для обеспечения его достоверности и эффективности.

Сравнение — это метод, при котором сопоставляются два или более объекта, явления или процесса, чтобы выявить их сходства и различия. Сравнение помогает определить уникальные характеристики и общие черты объектов, что может привести к новым открытиям и теоретическим обоснованиям.

Измерение — это процесс определения количественных характеристик объекта или явления. Измерение используется для получения точных данных, которые можно использовать для анализа и сравнения.

Индукция — метод логического вывода, при котором на основе наблюдения частных случаев формулируется общее правило или принцип.

Дедукция — это логический метод, при котором конкретные заключения делаются на основе общих принципов, аксиом или предположений. В процессе дедукции общие принципы или правила используются для получения специфических выводов о конкретных случаях. Этот метод позволяет проверять гипотезы и теории, делая выводы, исходя из установленной общей базы знаний.

Анализ — это процесс разделения сложного объекта или явления на более простые компоненты с целью детального изучения каждого из них. Этот процесс помогает понять, как отдельные части взаимодействуют друг с другом и как они влияют на целое. Анализ позволяет выделить ключевые элементы и выявить внутренние связи и зависимости.

Синтез — это процесс объединения отдельных элементов или идей в целостную структуру или систему. Этот метод помогает создавать новые концепции, теории или модели на основе уже существующих данных или знаний.

Гипотеза — это предварительное предположение или предположительное объяснение некоторого явления или процесса, которое требует проверки. Она формулируется на основе имеющихся данных или наблюдений и служит исходной точкой для дальнейшего научного исследования. Должна быть возможность её опровержения или подтверждения в ходе исследования.

Концепция — это обобщённое представление или система идей, которая объясняет определённое явление или проблему. Концепция включает

в себя основную теорию и ключевые принципы, которые объединяют различные гипотезы и исследования в целостное понимание предмета.

Соотношение — это связь между различными переменными, элементами или явлениями исследуемого объекта, которая показывает, как они взаимодействуют или влияют друг на друга. Соотношение помогает понять, как один элемент влияет на другой и как они взаимосвязаны.

Объект исследования — это конкретная изучаемая область реальности. Это может быть физический предмет, явление, процесс или система, которая становится предметом научного анализа. Объект исследования задаёт рамки исследования и определяет, что именно будет изучаться и какие аспекты будут исследованы.

Предмет исследования — это более узкий аспект или характеристика объекта исследования, на которую сосредоточено внимание. Это конкретные свойства, явления, которые будут изучаться в рамках более общего объекта. Предмет исследования помогает уточнить, какие именно вопросы будут решаться и какие аспекты будут анализироваться.

Методика исследования — это система методов и подходов, которые используются для проведения научного исследования. Она включает в себя конкретные способы сбора данных, их анализа и интерпретации. Методика исследования определяет, как будет проводиться работа, какие инструменты и техники будут применяться, и как результаты будут проверяться и документироваться.

Задание 3. На основе своего варианта определить:

основные компоненты научного исследования - его объекта, предмета анализа, задачи (или проблемы) исследования, совокупности исследовательских средств, необходимых для решения задачи заданного типа, а также сформировать представление о последовательности движения исследователя в процессе решения задачи.

1. Объект исследования

Объект исследования: Процессы обеспечения информационной безопасности, основанные на контроле и анализе поведения субъектов доступа (пользователей) в информационной системе.

2. Предмет анализа

Предмет анализа: Методы, модели и организационно-технические аспекты внедрения систем анализа поведения пользователей (User and Entity Behavior Analytics, UEBA) для выявления аномалий и признаков несанкционированного доступа.

3. Проблема исследования

Проблема исследования: существует противоречие между высоким потенциалом технологий анализа поведения пользователей для проактивного предотвращения угроз и сложностями их практического внедрения, связанными с точностью анализа, большим объемом ложных срабатываний, вопросами производительности и сохранения приватности данных.

Основная задача: оценить перспективы и разработать рекомендации по эффективному внедрению систем анализа поведения пользователей для повышения уровня защищенности от несанкционированного доступа.

Конкретные задачи (примеры):

1. Провести анализ современных угроз информационной безопасности, против которых эффективны системы анализа поведения.
2. Систематизировать и классифицировать существующие методы и модели анализа поведения пользователей (от простых статистических до машинного обучения).
3. Выявить ключевые критерии эффективности (точность, быстродействие, масштабируемость) и барьеры (ложные срабатывания, стоимость, приватность) внедрения таких систем.
4. Разработать модель (или критерии) для сравнительного анализа и выбора решения UEBA под конкретные задачи организации.
5. Сформулировать практические рекомендации по этапам внедрения и интеграции UEBA в существующую инфраструктуру безопасности.

4. Совокупность исследовательских средств

1. **Теоретические методы:**
   a. Системный анализ: Рассмотрение системы безопасности как целостного комплекса, где UEBA является одним из компонентов.
   b. Анализ и синтез: Анализ научной литературы, стандартов (например, NIST), материалов поставщиков решений. Синтез полученных знаний в единую модель.
   c. Классификация: Классификация методов анализа поведения, типов аномалий, архитектур систем.
   d. Сравнительный анализ: Сравнение различных подходов (например, основанных на правилах vs. на машинном обучении) по выделенным критериям.

2. **Эмпирические и практические методы:**
   a. Case-study (анализ кейсов):Изучение и анализ открытых случаев успешного и неудачного внедрения UEBA в реальных компаниях.

5. **Последовательность движения исследователя (Этапы исследования)**

Этап 1. Подготовительно-проектный:

1. Формулировка проблемы, цели, задач.
2. Составление плана и календарного графика исследования.
3. Проведение первоначального обзора научной литературы и рынка решений.

Этап 2. Теоретико-аналитический:

1. Глубокий систематизированный обзор литературы по теме: UEBA, машинное обучение для безопасности, инсайдерские угрозы.
2. Анализ и классификация существующих методов и архитектур.
3. Формирование теоретической базы исследования (определение ключевых понятий, критериев оценки).

Этап 3. Практико-моделирующий:

1. Сравнительный анализ существующих решений на основе разработанной модели.
2. Моделирование сценариев (или анализ кейсов) для верификации теоретических выводов.

Этап 4. Заключительно-обобщающий:

1. Обобщение полученных результатов.
2. Формулировка выводов о перспективах внедрения и разработка практических рекомендаций.
3. Оформление текста научной работы (статьи, отчета).
4. Подготовка презентации и представление результатов.

Контрольные вопросы

1. Что такое научное исследование?

Научное исследование — это экспериментальная или теоретическая деятельность, направленная на получение новых знаний об основных закономерностях строения, функционирования и развития человека, общества, окружающей среды.

2. Какие исследования относят к фундаментальным, а какие — к прикладным?

Фундаментальные исследования - направлены на получение новых знаний и теоретическое понимание закономерностей природы, общества или мышления без прямого расчета на практическое применение. Примеры: исследования в области теоретической физики, космологии.

Прикладные исследования - направлены на использование существующих теоретических знаний для решения конкретных практических задач. Они сосредоточены на разработке новых технологий, методов или процессов, которые могут быть непосредственно применены в практике.

3. Перечислите этапы научного исследования.

1. Определение проблемы.
2. Актуальность исследования.
3. Обзор источников и существующих данных.
4. Формулирование гипотезы.
5. Планирование задач для решения проблемы.
6. Исследование решений.
7. Анализ данных (сравнение с гипотезой).
8. Вывод.
9. Оформление результатов и публикация.

4. В чем состоит различие между прикладной и научной проблемой?

Научная проблема — это вопрос или задача, требующая исследования и анализа для получения нового знания или понимания в какой-либо области науки. Она обычно связана с поиском ответов на фундаментальные вопросы о закономерностях и принципах, которые управляют явлениями и процессами в природе или обществе. Решение научной проблемы может включать разработку новых теорий, моделей или методов, которые расширяют существующее знание и способствуют прогрессу в науке.

Прикладная проблема — это практическая задача, решение которой нацелено на улучшение или создание новых технологий, продуктов или процессов. Решение прикладной проблемы обычно ориентировано на достижение практических результатов и улучшение функциональности, эффективности или удобства в различных областях.

5. Как соотносятся между собой объект и предмет исследования?

Объект исследования — это конкретная изучаемая область реальности. Это может быть физический предмет, явление, процесс или система, которая становится предметом научного анализа. Объект исследования задаёт рамки исследования и определяет, что именно будет изучаться и какие аспекты будут исследованы.

Предмет исследования — это более узкий аспект или характеристика объекта исследования, на которую сосредоточено внимание. Это конкретные свойства, явления, которые будут изучаться в рамках более общего объекта. Предмет исследования помогает уточнить, какие именно вопросы будут решаться и какие аспекты будут анализироваться.

Объект исследования задает общие рамки и контекст, в котором проводится работа, а предмет исследования уточняет, на что конкретно будет направлено внимание в рамках этого объекта.

6. Какая информация фиксируется в рабочем плане научного исследования?

1. Тема и цель исследования.
2. Объект и предмет исследования.
3. Гипотезы.
4. Методы исследования.
5. План работ и сроки.
6. Ресурсы и материалы.
7. Ожидаемые результаты.
8. Источники.

7. Назовите основные требования, предъявляемые к результатам научного исследования.

1. **Новизна:** результаты должны представлять собой новый вклад в науку, предоставляя оригинальные находки или новые теоретические и практические подходы.
2. **Обоснованность**: результаты должны основываться на надежных и проверенных данных. Выводы должны быть логично выведены из проведенного исследования.
3. Достоверность: результаты должны быть проверены и воспроизводимы другими исследователями.
4. **Актуальность**: результаты должны быть значимыми для текущих научных и практических вопросов, отражая современные тенденции и потребности.
5. **Релевантность**: результаты должны соответствовать целям и задачам исследования, отвечая на поставленные вопросы и гипотезы.
6. Объективность: результаты не должны зависеть от субъективных факторов.
7. **Теоретическая и/или практическая значимость:** исследование должно либо расширять научные знания, либо иметь практическую ценность.
8. **Логичность и последовательность:** выводы должны быть обоснованными и логически вытекающими из анализа данных.

8. Приведите примеры научных результатов из сферы информационной безопасности, криптографии.

1. Разработка и внедрение протокола HTTPS.
2. Разработка алгоритма RSA для шифрования и цифровых подписей.
3. Разработка и внедрение алгоритма DES
4. Разработка и внедрение алгоритма «Магма»
5. Разработка и внедрение алгоритма «Кузнечик»