МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания по выполнению лабораторных работ по дисциплине

«Кибербезопасность мультиагентных робототехнических систем»

для студентов направления подготовки 10.04.01 «Информационная безопасность»
Направленность (профиль) «Информационная безопасность киберфизических систем»
Квалификация выпускника магистр

Ставрополь, 2026 г.

СОДЕРЖАНИЕ

Введение

Целью освоения дисциплины «Кибербезопасность мультиагентных робототехнических систем» является формирование профессиональных компетенций будущего магистра по направлению подготовки 10.04.01 «Информационная безопасность», направленность (профиль) «Информационная безопасность киберфизических систем» и формирование у обучающихся комплекса теоретических знаний и практических навыков, необходимых для выявления, анализа и нейтрализации угроз информационной безопасности в распределенных мультиагентных робототехнических системах, а также для разработки и применения методов и средств защиты таких систем на всех этапах их жизненного цикла.

Основными задачами дисциплины является: теоретическое и практическое освоение основных понятий и методов работы по следующим направлениям:

– архитектура и принципы функционирования мультиагентных робототехнических систем;

– классификация угроз информационной безопасности, характерные для мультиагентных систем, включая атаки на консенсус, состязательные атаки, атаки, основанные на внутренней модели, а также методы социальной инженерии, направленные на подрыв доверия между агентами;

– современные методы и модели обеспечения безопасности, включая системы доверия и репутации, механизмы обнаружения вторжений и аномалий, а также криптографические методы защиты каналов связи и хранимых данных в мультиагентных системах;

– методологии и стандарты, направленные на обеспечение устойчивости к атакам и гарантированное выполнение целевых функций системы в условиях деструктивных воздействий;

– применение методов анализа защищенности, конфигурирования средств защиты, а также использование мультиагентных подходов для решения задач кибербезопасности.

Дисциплина входит в часть учебного плана, формируемую участниками образовательных отношений дисциплины по выбору (Б1.В.ДВ.01.01) и адресована магистрам, обучающимся по направлению подготовки 10.04.01 «Информационная безопасность», направленность (профиль) «Информационная безопасность киберфизических систем». Особенность дисциплины в том, что она изучает комплексные проблемы обеспечения информационной безопасности в децентрализованных, самоорганизующихся гетерогенных системах коллективного взаимодействия роботов, где угрозы возникают не только на уровне отдельных агентов, но и на уровне их кооперативного поведения и эмерджентных эффектов.

Компетенции обучающегося, формируемые в результате освоения дисциплины

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций, индикаторов
ПК-1 Способен проводить исследования и анализ информационных процессов защиты информации в киберфизических системах	ИД-1 ПК-1 технологии поиска, изучения, обобщения, классификации и систематизации научной информации, методы анализа и обоснования выбора решений по обеспечению требуемого уровня безопасности информационных процессов защиты информации в киберфизических системах	Перечисляет и кратко характеризует этапы научного исследования применительно к анализу информационных процессов защиты информации в киберфизических системах
	ИД-2 ПК-1 применение современных информационных технологий и программных средств, при решении задач профессиональной деятельности	Обрабатывает полученные в ходе исследования данные и делает обоснованные заключения о защищённости системы
	ИД-4 ПК-1 применяет технологии исследования и анализа информационных процессов защиты информации в киберфизических системах	Подготавливает отчёт по результатам исследования (включая постановку, описание методологии, полученные данные, выводы и рекомендации) и представляет его для обсуждения в учебной группе или на научном семинаре

ТЕМА 1: Принципы функционирования мультиагентных робототехнических систем

ЛАБОРАТОРНАЯ РАБОТА №1

Тема: Архитектуры и принципы взаимодействия в мультиагентных робототехнических системах

Цель: изучить основные архитектуры (централизованная, децентрализованная, иерархическая) и протоколы взаимодействия агентов, а также освоить базовое конфигурирование симулятора роя.

Актуальность: Понимание архитектуры МРТС необходимо для выявления точек уязвимости и проектирования защитных механизмов; большинство атак реализуется через каналы взаимодействия агентов.

Теоретическая часть: Мультиагентные робототехнические системы состоят из множества автономных агентов, которые взаимодействуют для достижения общей цели. Архитектура определяет, как распределены управление и коммуникация. Централизованная архитектура имеет единый координатор, что упрощает принятие решений, но создаёт единую точку отказа. Децентрализованная (одноранговая) архитектура повышает живучесть, но требует сложных протоколов консенсуса. Иерархическая сочетает уровни управления. Для взаимодействия агенты используют протоколы обмена сообщениями (например, ROS Topics, ZeroMQ). В симуляции роев часто применяются модели «лидер-ведомый» или «стайное поведение» (boids). Ключевым параметром является частота обмена данными и задержка, влияющие на безопасность. Агенты могут обмениваться информацией о своем состоянии, сенсорных данных, командах. Без защиты такой обмен уязвим для подмены и прослушивания. Изучение архитектур позволяет в дальнейшем выбирать методы аутентификации и контроля целостности. Для практической работы используется симулятор ROS (Robot Operating System) с пакетом turtlesim или Gazebo с несколькими роботами.

Задания на лабораторную работу:

1. Запустить симулятор с тремя агентами в децентрализованной архитектуре и проанализировать потоки сообщений между ними.
2. Модифицировать конфигурацию так, чтобы один агент стал центральным координатором, и сравнить трафик.

Детализация выполнения:

- Установить ROS Noetic (или Melodic) и пакет turtlebot3_gazebo.
- Запустить симуляцию трёх роботов TurtleBot3 в среде Gazebo с использованием файла запуска turtlebot3_world.launch.
- С помощью команды rostopic list и rostopic info определить топики, используемые для обмена данными (например, /tb3_0/cmd_vel, /tb3_0/odom).
- Запустить анализатор трафика rqt_graph для визуализации взаимодействий между узлами.
- Для задания 2: изменить файл .launch, добавив параметр, назначающий одного робота лидером (например, через launch-аргумент leader:=true), и перезапустить симуляцию.

- Зафиксировать в отчёте: список топиков до и после изменения, схему взаимодействия, вывод о различиях в количестве сообщений и структуре связей.

ЛАБОРАТОРНАЯ РАБОТА №2

Тема: Самоорганизация и эмерджентное поведение в роевых системах

Цель: Изучить механизмы самоорганизации агентов на основе локальных правил и выявить потенциальные точки вмешательства злоумышленника.

Актуальность: Эмерджентное поведение (возникновение глобального интеллекта из локальных взаимодействий) может быть нарушено внедрением дезинформации или «роботов-предателей».

Теоретическая часть: Самоорганизация в МРТС позволяет агентам без центрального управления решать сложные задачи: построение формации, поиск цели, распределённая транспортировка. Классический алгоритм — Boids (правила сближения, выравнивания скорости, избегания столкновений). Другой пример — моделирование муравьиного алгоритма (феромонные пути). В кибербезопасности эмерджентность создаёт скрытые уязвимости: небольшое число скомпрометированных агентов может изменить коллективное решение (эффект «византийских генералов»). Атака может быть незаметной на локальном уровне, но приводить к глобальному сбою. Для исследования таких эффектов используются симуляторы массового роя (например, Buzz, ARGoS, или Python-библиотека pygame с реализацией Boids). Важно научиться детектировать аномалии в коллективном поведении по отклонениям от ожидаемой самоорганизации. В работе предстоит реализовать базовый рой с правилами Boids, затем ввести «агента-нарушителя», который нарушает правила сближения или передаёт ложные координаты.

Задания на лабораторную работу:

1. Реализовать на Python симуляцию роя из 10 агентов с алгоритмом Boids и визуализацией.
2. Внедрить одного вредоносного агента, который игнорирует правило избегания столкновений (целенаправленно таранит соседей), и зафиксировать влияние на среднее расстояние между агентами.

Детализация выполнения:

1. Использовать библиотеку pygame и написать класс Agent с атрибутами position, velocity, max_speed.
2. Реализовать три правила: разделение (избегание), сближение (движение к центру соседей), выравнивание скорости.
3. Добавить поле зрения (радиус взаимодействия).
4. Для задания 1: запустить симуляцию на 100 итераций, сохранить траектории.
5. Для задания 2: изменить метод update вредоносного агента так, чтобы его вектор желаемой скорости был направлен на ближайшего соседа с удвоенной силой.

6. Собрать статистику: среднее расстояние между всеми агентами в каждом кадре, построить график.

7. В отчёте представить код, скриншоты визуализации (начало, после атаки) и вывод о том, как один агент нарушает коллективное поведение.

ЛАБОРАТОРНАЯ РАБОТА №3

Тема: Протоколы обмена сообщениями и их уязвимости в МРТС

Цель: Изучить распространённые протоколы (ROS Topics, MQTT, CoAP) и провести анализ их защищённости применительно к мультиагентному взаимодействию.

Актуальность: Открытость протоколов (особенно ROS по умолчанию) без шифрования и аутентификации делает МРТС крайне уязвимой для подмены команд и перехвата данных.

Теоретическая часть: В МРТС для обмена данными часто используются легковесные протоколы. ROS (Robot Operating System) использует TCP/IP и собственный протокол TCPROS, который не шифрует сообщения и не аутентифицирует узлы по умолчанию. Любой узел в сети может подписаться на любой топик или публиковать ложные сообщения. MQTT – протокол publish/subscribe, может работать с TLS, но часто применяется без него. CoAP (Constrained Application Protocol) для IoT может использовать DTLS. Уязвимости включают: подслушивание (eavesdropping), подмена публикаций (spoofing), атака «отказ в обслуживании» путём флуда сообщениями, внедрение вредоносных узлов. В распределённой системе без центрального брокера (например, ROS без master) атаки ещё сложнее обнаружить. Для практического исследования предлагается использовать эмуляцию сети с помощью инструментов (Wireshark, tc) и утилит для генерации ложных сообщений. Студенты должны научиться перехватывать и модифицировать трафик между агентами.

Задания на лабораторную работу:

1. Запустить двух агентов в ROS, обменивающихся сообщениями через топик /data, перехватить трафик с помощью Wireshark и извлечь содержимое сообщений.

2. Используя утилиту rostopic pub, отправить ложное сообщение от имени одного агента другому и продемонстрировать приём ложных данных.

Детализация выполнения:

1. Установить ROS, запустить roscore.

2. Создать пакет с двумя узлами: publisher (публикует строку "Agent1 message") и subscriber (выводит в консоль).

3. Запустить Wireshark, выбрать интерфейс loopback (или Ethernet), фильтр tcp.port = 11311 (порт ROS master).

4. Захватить пакеты, найти TCP-поток с данными сообщения, убедиться, что строка передаётся в открытом виде.

5. Для задания 2: найти имя топика и тип сообщения (например, std_msgs/String). Выполнить команду: rostopic pub /data std_msgs/String "data: 'Fake command'" -r 1

6. Наблюдать, что подписчик принимает ложное сообщение как легитимное.

7. В отчёте указать: команды, скриншоты Wireshark, объяснение, почему такая уязвимость опасна для МРТС.

ТЕМА 2: Классификация угроз информационной безопасности мультиагентных робототехнических систем

ЛАБОРАТОРНАЯ РАБОТА №4

Тема: Классификация угроз информационной безопасности МРТС: физический уровень

Цель: Изучить угрозы физического уровня (захват робота, повреждение сенсоров, электромагнитное воздействие) и методы их частичной детекции.

Актуальность: В реальных МРТС физический захват агента злоумышленником позволяет извлечь ключи, модифицировать прошивку и использовать робота для внутренних атак.

Теоретическая часть: Угрозы физического уровня делятся на: захват устройства (capture), повреждение сенсоров (ослепление камеры, глушение GPS), подмена сенсорных данных через внешнее воздействие (например, лазер на лидар), энергетические атаки (отключение питания). При захвате робота злоумышленник может получить доступ к его памяти, включая криптографические ключи, и затем использовать этого робота как «троянского коня» внутри роя. Обнаружить физический захват можно через аномалии в поведении: неожиданное изменение траектории, нештатное энергопотребление, потеря связи. Также применяются механизмы «живучести» – если рой теряет связь с агентом, другие агенты могут начать его избегать. В лабораторной работе мы смоделируем захват агента и изменение его поведения в симуляции, а также реализуем простое детектирование на основе анализа позиции.

Задания на лабораторную работу:

1. В симуляции роя (из работы №2) реализовать «захват» одного агента: его координаты перестают обновляться нормально, он начинает двигаться случайным образом.

2. Реализовать детектор аномалий на основе сравнения предсказанной позиции (по предыдущей скорости) с фактической; при превышении порога считать агента скомпрометированным и исключить из взаимодействия.

Детализация выполнения:

1. Взять код Boids из ЛР№2. Добавить переменную compromised = False для одного агента.

2. В основном цикле: для скомпрометированного агента вместо правил Boids задать случайное ускорение.

3. Реализовать функцию predict_position(agent, dt), которая по последней скорости вычисляет ожидаемую позицию.

4. Каждый агент (кроме подозреваемого) сравнивает фактическое положение соседа с предсказанным. Если евклидово расстояние превышает

порог (например, 2 * max_speed * dt), то агент помечает соседа как «подозрительный».

5. При накоплении 3 голосов от разных агентов, подозрительный исключается из списка соседей для расчёта правил (игнорируется).

6. Запустить симуляцию с захваченным агентом, показать, как остальные перестают на него реагировать.

7. В отчёте описать логику детектирования, привести графики траекторий до и после исключения.

ЛАБОРАТОРНАЯ РАБОТА №5

Тема: Классификация угроз: коммуникационный уровень (атаки на каналы связи)

Цель: Изучить атаки на уровне сетевых протоколов (подмена MAC, ARP-spoofing, десинхронизация) и освоить базовые средства защиты (MACsec, статические ARP).

Актуальность: В беспроводных сетях МРТС атаки на коммуникационный уровень могут нарушить взаимодействие всей группы без физического доступа к роботам.

Теоретическая часть: Коммуникационные угрозы включают: подмену MAC-адреса (спуфинг) для выдачи себя за другой узел; ARP-spoofing для перенаправления трафика; атаки на протоколы маршрутизации (например, RPL в 6LoWPAN); глушение (jamming) радиоканала; атака «дезинформация о соседях» (отправка ложных beacon-сообщений). В проводных сетях также возможны атаки на STP (Spanning Tree) или VLAN hopping. Для защиты применяются: шифрование на канальном уровне (MACsec, 802.1AE), использование статических ARP-таблиц, протоколы с аутентификацией (RPL с Secure Neighbor Discovery). В лабораторной работе мы смоделируем ARP-spoofing в эмуляторе сети (Mininet) с участием нескольких виртуальных агентов и реализуем защиту.

Задания на лабораторную работу:

1. В Mininet создать сеть из 4 хостов (агентов) и коммутатора; запустить ARP-spoofing атаку с одного хоста, подменив IP-адрес другого.

2. Настроить статические ARP-записи на всех хостах и убедиться, что атака блокируется.

Детализация выполнения:

1. Установить Mininet, написать топологию: sudo mn --topo linear,4.

2. На хостах h1, h2, h3, h4 запустить простой UDP-чат (netcat).

3. С хоста h2 выполнить arpspoof -i h2-eth0 -t h1 -r h3 (подмена, чтобы h1 думал, что h3 — это h2).

4. Проверить перехват трафика с помощью tcpdump.

5. Для защиты: на каждом хосте выполнить arp -s <IP> <MAC> для всех соседей.

6. Повторить атаку – убедиться, что подмена не проходит.

7. В отчёте описать принцип ARP-spoofing, привести команды и скриншоты захвата пакетов.

ЛАБОРАТОРНАЯ РАБОТА №6

Тема: Атаки на уровне приложений: дезинформация и внедрение ложных целей

Цель: Изучить сценарии атак, при которых злоумышленник внедряет в рой ложные сенсорные данные (фиктивные цели, препятствия) и анализировать последствия.

Актуальность: МРТС часто полагаются на обмен картами, позициями целей; подмена этих данных может привести к столкновениям, уводящим агентов от истинной цели.

Теоретическая часть: На прикладном уровне атаки направлены на семантику данных. Например, в задаче патрулирования злоумышленник может публиковать сообщение об обнаружении цели, которой нет, чтобы отвлечь рой. Или наоборот, скрывать реальную цель. В распределённой системе без централизованной верификации такие атаки трудно обнаружить. Методы защиты: криптографическая аутентификация источников данных, консенсусные механизмы (голосование), проверка непротиворечивости с сенсорами самого агента. В лабораторной работе мы реализуем сценарий, где группа агентов ищет источник тепла. Один агент скомпрометирован и публикует ложные координаты «тепловой точки».

Задания на лабораторную работу:

1. Реализовать симуляцию 5 агентов, которые с помощью алгоритма роя ищут цель (одна статическая точка).
2. Внедрить одного агента-дезинформатора, который публикует в общем топике ложные координаты цели, смещённые на 10 единиц. Оценить отклонение роя от истинной цели.

Детализация выполнения:

1. На Python создать класс Agent с полями position, target_estimate (общее мнение).
2. Использовать простейший алгоритм: каждый агент измеряет расстояние до цели (если в радиусе обнаружения) и публикует свою оценку. Все агенты усредняют полученные оценки для движения.
3. Визуализация через matplotlib.
4. Для задания 2: у одного агента метод publish_target() возвращает координаты (true_target.x + 10, true_target.y + 10).
5. Запустить 100 итераций, записать траектории всех агентов.
6. Построить график ошибки (расстояние от каждого агента до истинной цели) для чистого сценария и с дезинформатором.
7. В отчёте объяснить, почему усреднение не спасает, если доля ложных сообщений высока.

ТЕМА 3: Современные методы и модели обеспечения информационной безопасности мультиагентных робототехнических систем

ЛАБОРАТОРНАЯ РАБОТА №7

Тема: Модели доверия и репутации для защиты от внутренних нарушителей

Цель: Изучить модели доверия на основе истории взаимодействий и реализовать простой репутационный механизм для выявления агентов-предателей.

Актуальность: Криптографическая аутентификация не защищает от легитимного, но скомпрометированного агента; модели доверия позволяют снизить влияние таких узлов.

Теоретическая часть: Модель доверия (trust model) оценивает надёжность агента на основе его предыдущего поведения. Репутация может вычисляться как средняя оценка за последние N взаимодействий. Агент, который часто даёт ложные показания, получает низкую репутацию, и его сообщения либо игнорируются, либо имеют меньший вес при голосовании. Существуют децентрализованные модели (каждый агент ведёт свою таблицу репутации) и централизованные. Важно защитить саму репутацию от подделки (например, цифровая подпись оценок). В лабораторной работе мы реализуем децентрализованную модель, где каждый агент оценивает других по точности переданных координат цели. При низкой репутации сообщения отбрасываются.

Задания на лабораторную работу:

1. Расширить симуляцию из ЛР№6, добавив для каждого агента словарь репутации соседей (начальное значение 1.0).
2. Реализовать механизм обновления репутации: после получения сообщения от соседа агент сравнивает его с собственным измерением (если оно есть); при совпадении (в пределах порога) репутация увеличивается, иначе уменьшается. Сообщения от агентов с репутацией ниже 0.3 игнорируются. Продемонстрировать, что дезинформатор быстро теряет влияние.

Детализация выполнения:

1. В коде агента добавить reputation = {agent_id: 1.0 for agent_id in agents}.
2. При получении сообщения о цели: если reputation[sender] > 0.3, то учитывать его в усреднении.
3. Если у агента есть собственное измерение цели (в радиусе сенсора), то он вычисляет разницу между полученной координатой и своей. Если разница < threshold (например, 1.0), то reputation[sender] += 0.1, иначе -= 0.1.
4. Ограничить репутацию в [0,1].
5. Запустить симуляцию с дезинформатором; вывести график изменения репутации дезинформатора у каждого из остальных агентов.
6. Показать, что траектории роя приближаются к истинной цели, несмотря на атаку.

7. В отчёте описать формулу обновления и пороги.

ЛАБОРАТОРНАЯ РАБОТА №8

Тема: Консенсусные алгоритмы для отказоустойчивости МРТС (PBFT, Raft)

Цель: Изучить алгоритмы достижения консенсуса в распределённой системе с возможными византийскими ошибками и реализовать упрощённый протокол голосования.

Актуальность: В МРТС без центрального координатора необходимо согласовывать общие решения (куда двигаться, какую цель атаковать) даже при наличии скомпрометированных агентов.

Теоретическая часть: Классическая проблема византийских генералов требует, чтобы честные узлы пришли к единому решению, даже если часть узлов передаёт противоречивую информацию. Алгоритм PBFT (Practical Byzantine Fault Tolerance) может выдерживать до f = (n-1)/3 злоумышленников. Raft обеспечивает консенсус только при crash-отказах (не византийских). Для роевых систем часто используют упрощённые протоколы, например, голосование с порогом (majority vote) и повторные раунды. Важно, чтобы агенты обменивались подписанными сообщениями. В лабораторной работе мы реализуем протокол согласования общей цели на основе голосования с цифровой подписью (эмулируя простую схему с общим секретным ключом).

Задания на лабораторную работу:

1. Реализовать протокол консенсуса для 5 агентов, где каждый предлагает свою координату цели. Агенты обмениваются предложениями и голосуют.
2. Внедрить двух византийских агентов, которые предлагают случайные координаты и голосуют непоследовательно. Показать, что при n=5, f=2 консенсус невозможен, а при добавлении ещё одного честного агента (n=7, f=2) – возможен.

Детализация выполнения:

1. Написать класс Agent с методом propose(), возвращающим координаты (честные – истинная цель, византийские – случайные).
2. Алгоритм:
3. Каждый агент широковещательно рассылает своё предложение.
4. Каждый собирает предложения в течение таймаута.
5. Каждый голосует за предложение, которое ближе к его собственному измерению (или просто выбирает наиболее частое).
6. Голоса рассылаются.
7. Агент принимает решение, если за какое-то предложение проголосовало более 2/3 агентов.
8. Эмулировать цифровую подпись: добавить поле signature = hash(proposal + secret_key) (упрощённо).
9. Проверить для n=5 (2 византийца) – консенсус не достигается (разные решения).
10. Добавить двух честных (n=7) – консенсус возможен.

11. В отчёте привести псевдокод и результаты моделирования.

ЛАБОРАТОРНАЯ РАБОТА №9

Тема: Методы шифрования и аутентификации в каналах M2M

Цель: Освоить применение легковесных криптографических алгоритмов (ChaCha20-Poly1305, HMAC-SHA256) для защиты сообщений между агентами в условиях ограниченных ресурсов.

Актуальность: Классические алгоритмы (RSA, AES-GCM) могут быть слишком тяжелыми для встраиваемых роботов; лёгковесные альтернативы обеспечивают баланс между безопасностью и производительностью.

Теоретическая часть: Для M2M-коммуникаций в МРТС требуются алгоритмы с низким потреблением энергии и малой задержкой. ChaCha20 – поточный шифр, быстрее AES на платформах без аппаратного ускорения. Poly1305 – код аутентификации сообщений. Вместе они образуют аутентифицированное шифрование (AEAD). HMAC на основе SHA256 также широко используется. В лабораторной работе мы реализуем безопасный канал между двумя агентами в симуляции: сообщения будут шифроваться, подписываться и проверяться. Будет использована библиотека cryptography на Python.

Задания на лабораторную работу:

1. Написать два скрипта (эмуляция агентов), обменивающихся сообщениями через сокеты с шифрованием ChaCha20-Poly1305.
2. Реализовать проверку целостности с помощью HMAC-SHA256 (без шифрования) и сравнить время выполнения на 10000 сообщений.

Детализация выполнения:

1. Установить pip install cryptography.
2. Для задания 1:
   - Генерировать 32-байтный ключ.
   - Использовать ChaCha20Poly1305(key) для шифрования/расшифровки.
   - Отправить зашифрованный nonce+ciphertext+tag по UDP.
3. Для задания 2:
   - Использовать HMAC(key, message, hashlib.sha256).
   - Замерить время через time.perf_counter().
4. Выполнить тесты на локальной машине.
5. В отчёте представить код, таблицу времени, вывод о применимости для реального времени в МРТС.

ЛАБОРАТОРНАЯ РАБОТА №10

Тема: Системы обнаружения вторжений (IDS) для мультиагентных систем

Цель: Изучить архитектуру распределённого IDS, где агенты наблюдают за поведением соседей, и реализовать простое правило детектирования аномалий.

Актуальность: Централизованный IDS имеет единую точку отказа; распределённый IDS повышает живучесть, но требует консенсуса по тревогам.

Теоретическая часть: В МРТС IDS может быть реализован как набор локальных агентов-мониторов, которые анализируют трафик и поведение. При обнаружении аномалии (например, слишком высокая частота сообщений, изменение траектории, несоответствие модели движения) монитор отправляет оповещение соседям. Для снижения ложных срабатываний применяется голосование. Также используются модели поведения, обученные на нормальных данных (машинное обучение). В лабораторной работе мы реализуем простой IDS на основе отклонения от нормальной модели движения – агент должен двигаться с ограниченным ускорением.

Задания на лабораторную работу:

1. В симуляции роя добавить мониторинг ускорения каждого агента; если ускорение превышает допустимое (например, в 2 раза больше обычного), генерируется событие.
2. Реализовать распределённый IDS: каждый агент сообщает соседям об аномалиях, и если более половины соседей согласны, то аномальный агент помечается и исключается.

Детализация выполнения:

1. Взять код Boids из ЛР№2. Добавить параметр max_acceleration.
2. В каждом цикле для каждого агента вычислять acceleration = (velocity_new - velocity_old)/dt.
3. Если |acceleration| > max_acceleration * 2, то агент (монитор) фиксирует аномалию у себя и рассылает сообщение «suspicion(agent_id)».
4. Каждый агент ведёт счётчик подозрений для каждого соседа. При получении suspicion от соседа увеличивает счётчик.
5. Если счётчик > (число соседей/2), то агент-нарушитель помечается и удаляется из роя (или игнорируется).
6. Протестировать, создав агента с внезапным рывком.
7. В отчёте описать правила детектирования и алгоритм консенсуса.

ЛАБОРАТОРНАЯ РАБОТА №11

Тема: Применение блокчейна для децентрализованной аутентификации агентов

Цель: Изучить возможности использования распределённого реестра для управления идентификаторами и ключами агентов в МРТС без единого центра.

Актуальность: В открытых роях новые агенты могут присоединяться динамически; блокчейн обеспечивает неизменяемую запись о легитимных агентах и их публичных ключах.

Теоретическая часть: Децентрализованная PKI на блокчейне (например, Ethereum с смарт-контрактами) позволяет регистрировать идентификаторы агентов и их открытые ключи. Каждый агент может проверить публичный ключ другого, обращаясь к блокчейну. Также возможна запись репутации. Однако блокчейн требует вычислительных ресурсов и

может быть медленным. Для лёгковесных МРТС используются упрощённые варианты (DAG, IOTA). В лабораторной работе мы используем эмуляцию блокчейна (например, локальную сеть Ganache) и напишем смарт-контракт для регистрации агентов.

Задания на лабораторную работу:

1. Развернуть локальную тестовую сеть Ethereum (Ganache) и написать смарт-контракт на Solidity для регистрации агентов (адрес Ethereum -> публичный ключ).
2. Реализовать клиент на Python (Web3.py), который позволяет агенту зарегистрироваться и получить публичный ключ другого агента по его идентификатору.

Детализация выполнения:

1. Установить Ganache CLI, создать сеть с 10 аккаунтами.
2. Написать контракт:

solidity

mapping(address => string) public pubkeys;

function register(string memory key) public { pubkeys[msg.sender] = key; }

function getKey(address agent) public view returns (string) { return pubkeys[agent]; }

3. Развернуть контракт через Truffle или Remix.
4. На Python использовать Web3, подключиться к Ganache, создать аккаунт, вызвать register("agent1_public_key").
5. Другой агент вызывает getKey(agent1_address).
6. Продемонстрировать, что ключ получен из блокчейна.
7. В отчёте описать преимущества и недостатки такого подхода для МРТС.

ТЕМА 4: Методологии и стандарты в области обеспечения информационной безопасности мультиагентных робототехнических систем

ЛАБОРАТОРНАЯ РАБОТА №12

Тема: Стандарты безопасности (IEC 62443) и их применение к МРТС

Цель: Изучить требования стандарта IEC 62443 к компонентам и системам, а также провести анализ соответствия простой МРТС этим требованиям.

Актуальность: IEC 62443 является базовым для промышленной кибербезопасности; умение применять его к робототехническим системам необходимо для сертификации.

Теоретическая часть: IEC 62443 состоит из нескольких частей: общие понятия (1-1), модель зон и каналов (1-2), требования к системам (3-3), требования к компонентам (4-2). Для МРТС важно определить зоны безопасности (например, зона управления, зона полевых устройств) и каналы между ними. Каждый агент может рассматриваться как компонент. Требования включают: идентификация и аутентификация (IAC), контроль доступа (AC), использование шифрования, целостность данных, ограничение

функциональности. В лабораторной работе студенты анализируют гипотетическую МРТС (рой дронов для инспекции трубопровода) и заполняют чек-лист соответствия.

Задания на лабораторную работу:

1. Изучить раздел IEC 62443-3-3 (требования к системе) и составить таблицу требований, применимых к МРТС.
2. Для заданного сценария (5 дронов, обмен по Wi-Fi, центральный пульт) провести gap-анализ: указать, какие требования выполнены, а какие нет, и предложить меры по их реализации.

Детализация выполнения:

1. Предоставить студентам выдержки из IEC 62443-3-3 (например, требования FR1-FR7).
2. Таблица: столбцы «Требование», «Реализовано? (да/нет/частично)», «Рекомендации».
3. Сценарий: дроны используют самоподписанные сертификаты, канал шифрован (WPA2), нет аутентификации на уровне приложения, нет системы обнаружения вторжений.
4. Студенты должны отметить отсутствие централизованного управления ключами, отсутствие журналирования, отсутствие защиты от подмены команд.
5. Предложить: внедрить PKI, добавить RADIUS-сервер, включить аудит, установить IDS.
6. В отчёте представить таблицу и список рекомендаций.

ЛАБОРАТОРНАЯ РАБОТА №13

Тема: Методология Security by Design для разработки защищённых МРТС

Цель: Освоить принципы безопасной разработки (моделирование угроз, анализ рисков, принцип наименьших привилегий) на примере проектирования простого роя.

Актуальность: Внедрение безопасности на поздних этапах разработки МРТС значительно дороже и менее эффективно; Security by Design позволяет закладывать защиту с самого начала.

Теоретическая часть: Security by Design включает: определение границ системы, построение модели угроз (например, с использованием STRIDE), анализ рисков (качественный/количественный), выбор контрмер, реализацию принципа наименьших привилегий, защиту по умолчанию, отказоустойчивость. Для МРТС особое внимание уделяется защите каналов связи и изоляции компонентов. В лабораторной работе студенты выступают в роли архитекторов, разрабатывающих спецификацию безопасности для новой системы.

Задания на лабораторную работу:

1. Для роя из 20 наземных роботов, работающих на открытой местности, построить модель угроз (перечислить активы, угрозы, уязвимости).

2. Разработать архитектурные решения, обеспечивающие безопасность, и обосновать их с точки зрения затрат/эффективности.

Детализация выполнения:

1. Активы: координаты роботов, команды управления, карта местности, ключи шифрования.
2. Угрозы: подмена GPS, захват робота, перехват команд, глушение.
3. Для каждой угрозы предложить контрмеру: использование криптографической аутентификации команд, аппаратные ключи в TPM, резервные каналы связи, детекция глушения.
4. Описать, как эти меры встраиваются в архитектуру: каждый робот имеет TPM, используется протокол с цифровой подписью, реализован distributed IDS.
5. В отчёте привести таблицу «Угроза – Контрмера – Оценка сложности реализации».

ЛАБОРАТОРНАЯ РАБОТА №14

Тема: Тестирование на проникновение (пентест) мультиагентной робототехнической системы в симуляции

Цель: Провести комплексную атаку на симулированную МРТС (сочетание подмены сообщений, захвата агента, дезинформации) и оценить эффективность защитных механизмов.

Актуальность: Реальные атаки часто являются комбинированными; умение проводить пентест помогает выявить слабые места в системе безопасности.

Теоретическая часть: Пентест МРТС включает этапы: разведка (сбор информации о протоколах, топологии), моделирование атак (нарушение целостности, доступности, конфиденциальности), анализ последствий. В симуляции можно безопасно испытывать деструктивные воздействия. Защитные механизмы включают: аутентификацию, шифрование, IDS, репутацию. В лабораторной работе студенты получают виртуальную среду с роем, в которой уже реализованы некоторые защитные меры (например, HMAC-аутентификация и IDS на основе ускорения). Задача – провести успешную атаку, обойдя эти меры, либо доказать, что система устойчива.

Задания на лабораторную работу:

1. В предоставленной симуляции (с защитой HMAC и IDS) попытаться скомпрометировать рой: либо нарушить его целостность, либо отклонить от цели.
2. По результатам атаки подготовить отчёт с описанием использованных методов и предложениями по усилению защиты.

Детализация выполнения:

1. Студентам выдаётся код симуляции (на основе ЛР№7, ЛР№10) с включённой аутентификацией HMAC и IDS.
2. Они могут модифицировать код атакующего агента, добавлять новые типы атак (например, атака повторного воспроизведения с записью легитимных сообщений, использование клонированного ID).

3. Разрешено также физическое глушение (эмуляция потери пакетов).

4. Студенты должны попытаться достичь хотя бы одного из эффектов: заставить рой сбиться с курса, столкнуться, уйти в запретную зону.

5. Если атака удалась – описать, почему защита не сработала. Если нет – доказать устойчивость.

6. В отчёте представить сценарий атаки, код изменений, графики траекторий до и после, выводы.

Рекомендуемая литература

Основная литература:

1. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под редакцией профессора РАН, доктора технических наук Д.П. Зегжды. – М.: Горячая линия – Телеком, 2020. – 560 с.: ил.

2. Коршунов, Г. И. К70 Сложные киберфизические системы: учеб. пособие / Г. И. Коршунов, И. А. Пастушок, А. А. Петрушевская. – СПб.: ГУАП, 2021. – 141 с.

3. E. A. Lee and S. A. Seshia, Introduction to Embedded Systems - A Cyber-Physical Systems Approach, Second Edition, MIT Press, 2017.

Дополнительная литература:

1. Грибунин В.Г., Мартынов А.П., Николаев Д.Б., Фомченко В.Н. Криптография и безопасность цифровых систем: Учебное пособие / Под ред.

2. Астайкина А.И. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2011, 411 с.

3. Защита информации в компьютерных системах и сетях. / В. Ф. Шаньгин, Москва: ДМК Пресс, 2012. – 592 с.: ил.

4. Информационная безопасность открытых систем [Электронный ресурс]: учебник / Д.А. Мельников. — 3-е изд., стер. — М.: ФлИнта, 2019. — 444 с.

5. Бабаш А.В. Криптографические методы защиты информации. Т. 1: учеб.-метод. пособие / А.В. Бабаш. — 2-е изд. — М.: РИОР: ИНФРА-М, 2018. — 413 с.

6. Криптография и безопасность в технологии .NET /П. Торстейнсон, Г.А. Ганеш; пер.с англ. — 4-е изд., электрон. — М.:Лаборатория знаний, 2020. — 482 с.

Интернет – ресурсы:

1. Официальный сайт Федеральной службы по техническому и экспортному контролю https://fstec.ru/

2. Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) https://rkn.gov.ru/

3. Официальный сайт Федеральной службы безопасности Российской Федерации http://www.fsb.ru/ -

4. Консультант Плюс - законодательство РФ кодексы и законы в последней редакции http://www.consultant.ru/

5. Интернет портал Защита-информации.SU http://www.iso27000.ru/

6. Научная электронная библиотека eLIBRARY.RU http://elibrary.ru

7. Консорциум сетевых электронных библиотек ЭБС «Лань» https://e.lanbook.com/

8. ЭБС «Университетская библиотека ОНЛАЙН» https://www.biblioclub.ru/ -

9. ЭБС IPR SMART https://www.iprbookshop.ru/

10. ЭБС Znanium https://znanium.com/

11. ЭБС «Юрайт» http://www.biblio-online.ru

12. Поисковые интернет-системы Яндекс, Rambler, Google и др.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания по выполнению самостоятельных работ по дисциплине

«Кибербезопасность мультиагентных робототехнических систем»

для студентов направления подготовки 10.04.01 «Информационная безопасность»
Направленность (профиль) «Информационная безопасность киберфизических систем»
Квалификация выпускника магистр

Ставрополь, 2026 г.

ВВЕДЕНИЕ

Самостоятельная работа студентов – важнейшая составная часть занятий, необходимая для полного усвоения программы курса.

Целью самостоятельной работы является закрепление и углубление знаний, полученных студентами на лекциях, подготовке к текущим практическим занятиям, промежуточным формам контроля знаний и к итоговому контролю.

Дидактические цели самостоятельных занятий:

- формирование профессиональных умений;
- формирование умений и навыков самостоятельного умственного труда;
- мотивирование регулярной целенаправленной работы по освоению специальности;
- развитие самостоятельности мышления;
- формирование убежденности, волевых черт характера, способности к самоорганизации;
- овладение технологическим учебным инструментом.

Самостоятельная работа включает те разделы курса, которые не получили достаточного освещения на лекциях по причине ограниченности лекционного времени и большого объема изучаемого материала.

Методическое обеспечение самостоятельной работы дисциплине состоит из:

1. Определения учебных вопросов, которые студенты должны изучить самостоятельно;
2. Подбора необходимой учебной литературы, обязательной для проработки и изучения;
3. Поиска дополнительной научной литературы, к которой студенты могут обращаться по желанию, если у них возникает интерес в данной теме;

4. Определения контрольных вопросов, позволяющих студентам самостоятельно проверить качество полученных знаний;
5. Организации консультаций преподавателя со студентами для разъяснения вопросов, вызвавших у студентов затруднения при самостоятельном освоении учебного материала.

Самостоятельная работа студента – это особым образом организованная деятельность, включающая в свою структуру такие компоненты, как:

- уяснение цели и поставленной учебной задачи;
- четкое и системное планирование самостоятельной работы;
- поиск необходимой учебной и научной информации;
- освоение собственной информации и ее логическая переработка;
- использование методов исследовательской, научно-исследовательской работы для решения поставленных задач;
- выработка собственной позиции по поводу полученной задачи;
- представление, обоснование и защита полученного решения;
- проведение самоанализа и самоконтроля.

Виды самостоятельных работ по учебной дисциплине:

- работа с понятийным аппаратом;
- поисковая работа с различными источниками;
- проектирование фрагментов исследовательской деятельности;
- анализ научных исследований по проблематике;
- подготовка докладов по теме.

Контроль знаний студентов включает формы текущего и итогового контроля. Текущий контроль осуществляется в процессе изучения курса и включает в себя оценку работы студентов на практических занятиях (дискуссии, заполнение и анализ таблиц, подготовка и проведение мини-исследований), а также подготовку домашнего задания.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ИЗУЧЕНИЮ ТЕОРЕТИЧЕСКОГО МАТЕРИАЛА

Лабораторные работы проводятся под руководством преподавателя. Чтобы хорошо подготовиться к практическому занятию, студенту необходимо:

- уяснить вопросы и задания, рекомендуемые для подготовки к практическому занятию;

- ознакомиться с методическими указаниями, которые представлены в каждом плане практического занятия;

- прочитать дополнительную литературу, рекомендованную преподавателем.

На студента обрушивается громадный объем информации, которую необходимо усвоить. Нужный материал содержится в учебниках, книгах, статьях. Порой возникает необходимость привлекать информационные ресурсы Интернет.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО РАБОТЕ С ЛИТЕРАТУРОЙ

При изучении дисциплины у студентов должен вырабатываться рационально-критический подход к изучаемым проблемам и явлениям. Это включает понимание того, что со временем ряд информационных и теоретических материалов устаревает, требуя критического отношения. С другой стороны, каждый текущий вопрос имеет свою историю, которую тоже полезно знать. Каждое событие может иметь разные интерпретации, поэтому слова, сказанные много лет назад, могут иметь важное значение.

Чтобы понять содержание материала, нужно уметь его прочитывать. Начинать следует с предварительного просмотра, в ходе которого ознакомиться с названием работы, с аннотацией, оглавлением, предисловием. Часто замысел работы ясен уже при ознакомлении с ее названием. Но особенно интересен просмотр оглавления, в результате которого становится

ясным развитие мысли автора. Неплохо было бы появившиеся при этом мысли зафиксировать на бумаге.

Просматривая текст оглавления, нужно остановиться на тех главах, которые представляют для вас особенный интерес, бегло ознакомиться с ними, составляя в общих чертах свое представление о них. Цель этого действия – найти места, относящиеся к искомой теме, определив при этом, что ценного в каждом из них.

Следующий этап – прочтение выделенных мест с фиксацией самых главных сведений. При этом надо четко и ясно осознавать цель чтения, постоянно держа ее перед собой: по какому вопросу нужна информация, для чего нужна, ее характер и т.д. необходимо менять режим чтения – от беглого вдумчивого – в зависимости от ценности информации, останавливаясь там, где это требуется для глубокого понимания текста.

Следует научиться определять структуру текста по соподчиненности его частей, учитывая взаимосвязь текста с рисунками, сносками, примечаниями и таблицами. Все это поможет пониманию текста при беглом ознакомлении с ним. Так вырабатывается способность при прочтении сразу понимать смысл и значение новой информации.

Многие книги и статьи имеют в своем аппарате списки литературы, которые дают возможность пополнить информационную осведомленность о дополнительной литературе по данному вопросу.

Отдельный этап прочтения – ведение записей прочитанного. Существует несколько видов записей: план, выписки, тезисы, аннотация, резюме, конспект.

Планом удобно пользоваться при подготовке к устному выступлению по выбранной теме. Каждый пункт плана должен раскрывать одну из сторон избранной темы, а весь план должен охватывать ее целиком.

Тезисы предполагают сжатое изложение основных положений текста в форме утверждения или отрицания. Они являются более совершенной формой записей и представляют основу для дискуссии. К тому же их легко запомнить.

Аннотация – краткое изложение содержания – дает общее представление о работе.

Резюме кратко характеризует выводы, главные итоги произведения.

Конспект является наиболее распространенной формой ведения записей. Основную ткань конспекта составляют тезисы, дополненные доказательствами и рассуждениями. Конспект может быть текстуальным, свободным или тематическим. Текстуальный представляет собой цитатник с сохранение логики работы и структуры текста. Свободный конспект основан на изложении материала в том порядке, который боле удобен автору. В этом смысле конспект представляет собирание воедино мыслей, разбросанных по всей книге. Тематический конспект может быть составлен по нескольким источникам, где за основу берется тема, интерпретируемая по-разному.

Экономию времени дает использование при записях различного рода сокращений, аббревиатуры и т.д. многие используют для регистрации исследуемых тем систему карточек. Преимущество карточек в том, что тема там излагается очень сжато, и они очень удобны в использовании, т.к. их можно разложить на столе, перегруппировать и без труда найти искомую тему.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО НАПИСАНИЮ И ОФОРМЛЕНИЮ ДОКЛАДА

Написание доклада по дисциплине является одним из видов самостоятельной работы студентов. Данный вид работы способствует повышению качества усвоения программного материала, углубленному пониманию наиболее сложных вопросов курса, расширению круга рассматриваемых проблем, овладению научными методами анализа психологических явлений.

Работая с литературными источниками, не следует ограничиваться простым пересказом содержания прочитанного. Необходимо выделить наиболее важные теоретические положения и обосновать их, раскрыть особенности различных точек зрения на один и тот же вопрос, оценить практическое и

теоретическое значение результатов реферируемой работы, а также выразить собственное отношение к идеям и выводам автора, подкрепив его определенными аргументами (личным опытом, высказываниями других исследователей и пр.).

Реферируемый источник, списки использованной литературы, а также все ссылки на литературные работы должны быть оформлены по алфавиту с указанием фамилии и инициалов автора, название источника, места и года издания; для журнальных статей необходимо указать фамилию и инициалы автора, название статьи, журнала, год издания и номер.

Доклад по дисциплине «……..»
студента ... курса (фамилия, имя, отчество)
группы
Тема: ".....".
год выполнения.

1. Общие положения

1.1. Доклад, как вид самостоятельной работы в учебном процессе, способствует формированию навыков исследовательской работы, расширяет познавательные интересы, учит критически мыслить.

1.2. При написании доклада по заданной теме студент составляет план, подбирает основные источники.

1.3. В процессе работы с источниками систематизирует полученные сведения, делает выводы и обобщения.

1.4. К докладу по крупной теме могут привлекать несколько студентов, между которыми распределяются вопросы выступления.

2. Выбор темы доклада

2.1. Тематика доклада обычно определяется преподавателем, но в определении темы инициативу может проявить и студент.

2.2. Прежде чем выбрать тему доклада, автору необходимо выявить свой интерес, определить, над какой проблемой он хотел бы поработать, более глубоко ее изучить.

3. Этапы работы над докладом

3.1. Формулирование темы, причем она должна быть не только актуальной по своему значению, но и оригинальной, интересной по содержанию.

3.2. Подбор и изучение основных источников по теме (как правильно, при разработке доклада используется не менее 8-10 различных источников).

3.3. Составление списка использованных источников.

3.4. Обработка и систематизация информации

3.5. Разработка плана доклада.

3.6. Написание доклада.

3.7. Публичное выступление с результатами исследования.

4. Структура доклада:

- титульный лист

- оглавление (в нем последовательно излагаются названия пунктов доклада, указываются страницы, с которых начинается каждый пункт);

- введение (формулирует суть исследуемой проблемы, обосновывается выбор темы, определяются ее значимость и актуальность, указываются цель и задачи доклада, дается характеристика используемой литературы);

- основная часть (каждый раздел ее, доказательно раскрывая отдельную проблему или одну из ее сторон, логически является продолжением предыдущего; в основной части могут быть представлены таблицы, графики, схемы);

- заключение (подводятся итоги или дается обобщенный вывод по теме доклада, предлагаются рекомендации);

- список использованных источников

5. Структура и содержание доклада

5.1. Введение - это вступительная часть научно-исследовательской работы. Автор должен приложить все усилия, чтобы в этом небольшом по объему

разделе показать актуальность темы, раскрыть практическую значимость ее, определить цели и задачи эксперимента или его фрагмента.

5.2. Основная часть. В ней раскрывается содержание доклада.

Как правило, основная часть состоит из теоретического и практического разделов.

В теоретическом разделе раскрываются история и теория исследуемой проблемы, дается критический анализ литературы и показываются позиции автора.

В практическом разделе излагаются методы, ход, и результаты самостоятельно проведенного эксперимента или фрагмента.

В основной части могут быть также представлены схемы, диаграммы, таблицы, рисунки и т.д.

5.3. В заключении содержатся итоги работы, выводы, к которым пришел автор, и рекомендации. Заключение должно быть кратким, обязательным и соответствовать поставленным задачам.

5.4. Список использованных источников представляет собой перечень использованных книг, статей, фамилии авторов приводятся в алфавитном порядке, при этом все источники даются под общей нумерацией литературы. В исходных данных источника указываются фамилия и инициалы автора, название работы, место и год издания.

5.5. Приложение к докладу оформляются на отдельных листах, причем каждое должно иметь свой тематический заголовок и номер, который пишется в правом верхнем углу, например: «Приложение 1»

6. Требования к оформлению доклада

6.1. Объем доклада может колебаться в пределах 5-15 печатных страниц; все приложения к работе не входят в ее объем.

6.2. Доклад должен быть выполнен грамотно, с соблюдением культуры изложения.

6.3. Обязательно должны иметься ссылки на используемую литературу.

6.4. Должна быть соблюдена последовательность написания библиографического аппарата.

7. Критерии оценки доклада

- актуальность темы исследования;

- соответствие содержания теме;

- глубина проработки материала; правильность и полнота использования источников;

- соответствие оформления доклада стандартам.

По усмотрению преподавателя доклады могут быть представлены на семинарах, научно-практических конференциях, а также использоваться как зачетные работы по пройденным темам.

Оценкой «отлично» оценивается доклад, в котором соблюдены следующие требования: полно и четко представлены основные теоретические понятия; проведен глубокий анализ по проблеме; продемонстрировано знание методологических основ изучаемой проблемы; уместно и точно использованы различные иллюстративные приемы – примеры, схемы, таблицы и т. д.; показано знание межпредметных связей; работа написана с использованием терминов современной науки, хорошим русским языком, соблюдена логическая стройность работы; соблюдены все требования к оформлению доклада.

Оценкой «хорошо» оценивается доклад, в которой: в целом раскрыта актуальность темы; в основном представлен обзор основной литературы по данной проблеме; недостаточно использованы последние публикации по данному вопросу; выводы сформулированы недостаточно полно; собственная точка зрения отсутствует или недостаточно аргументирована; в изложении преобладает описательный характер

Оценка «удовлетворительно» выставляется при условии: изложение носит исключительно описательный, компилятивный характер; библиография ограничена; изложение отличается слабой аргументацией; работа не выстроена логически; недостаточно используется научная терминология; выводы тривиальны; имеются существенные недостатки в оформлении.

Если большинство изложенных требований к докладу не соблюдено, то он не засчитывается.

Темы докладов

Базовый уровень

1. Основные архитектуры мультиагентных робототехнических систем: централизованная, децентрализованная, иерархическая.
2. Протоколы обмена сообщениями в МРТС (ROS, MQTT, CoAP) и их базовые уязвимости.
3. Классификация угроз информационной безопасности МРТС: физический, коммуникационный и прикладной уровни.
4. Атака «византийские узлы» в роевых системах: сущность и последствия.
5. Роль TPM и аппаратных модулей доверия в защите агентов МРТС.
6. Основы цифровой подписи и кодов аутентификации сообщений для защиты команд управления.
7. Принципы работы распределённых систем обнаружения вторжений (IDS) в рое.
8. Обзор стандарта IEC 62443 и его применимость к робототехническим системам.
9. Концепция доверия и репутации в МРТС: базовые модели.
10. Методы защиты от подмены сенсорных данных и дезинформации в мультиагентных системах.

Повышенный уровень

1. Устойчивость алгоритмов консенсуса (PBFT, Raft) к византийским атакам в роях с ограниченными ресурсами.
2. Децентрализованная PKI на основе блокчейна для динамической аутентификации агентов в открытых МРТС.
3. Атаки на самоорганизующиеся алгоритмы (Boids, муравьиные алгоритмы) и методы их обнаружения с помощью машинного обучения.

4. Легковесные постквантовые криптоалгоритмы для M2M-коммуникаций в мультиагентных системах.

5. Модели репутации на основе байесовского вывода и теории игр для противодействия внутренним нарушителям.

6. Методология Security by Design при разработке распределённых робототехнических систем: моделирование угроз STRIDE и анализ рисков.

7. Глушение (jamming) и защита от него в беспроводных роях: адаптивные схемы перестройки частоты и пространственное разделение.

8. Применение гомоморфного шифрования для агрегации сенсорных данных в МРТС без раскрытия индивидуальных показаний.

9. Стандарт ISO 10218 (роботы) и его пересечение с IEC 62443: требования к кибербезопасности коллаборативных роботов.

10. Тестирование на проникновение (пентест) мультиагентных систем: методы, инструменты и оценка последствий комбинированных атак.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОФОРМЛЕНИЮ ПРЕЗЕНТАЦИИ ДОКЛАДА

Мультимедийные презентации используются для того, чтобы выступающий смог на большом экране или мониторе наглядно продемонстрировать дополнительные материалы к своему сообщению.

Чтобы презентация хорошо воспринималась слушателями и не вызывала отрицательных эмоций (подсознательных или вполне осознанных), необходимо соблюдать правила ее оформления.

Презентация предполагает сочетание информации различных типов: текста, графических изображений, музыкальных и звуковых эффектов, анимации и видеофрагментов. Поэтому необходимо учитывать специфику комбинирования фрагментов информации различных типов. Кроме того, оформление и демонстрация каждого из перечисленных типов информации также подчиняется определенным правилам. Так, например, для текстовой

информации важен выбор шрифта, для графической — яркость и насыщенность цвета, для наилучшего их совместного восприятия необходимо оптимальное взаиморасположение на слайде.

Рекомендации по оформлению и представлению на экране материалов различного вида.

Текстовая информация

- размер шрифта: 24–54 пункта (заголовок), 18–36 пунктов (обычный текст);
- цвет шрифта и цвет фона должны контрастировать (текст должен хорошо читаться);
- тип шрифта: для основного текста гладкий шрифт без засечек (Arial, Tahoma, Verdana), для заголовка можно использовать декоративный шрифт, если он хорошо читаем;
- курсив, подчеркивание, жирный шрифт, прописные буквы рекомендуется использовать только для смыслового выделения фрагмента текста.

Графическая информация

- рисунки, фотографии, диаграммы призваны дополнить текстовую информацию или передать ее в более наглядном виде;
- желательно избегать в презентации рисунков, не несущих смысловой нагрузки, если они не являются частью стилевого оформления;
- цвет графических изображений не должен резко контрастировать с общим стилевым оформлением слайда;
- иллюстрации рекомендуется сопровождать пояснительным текстом;
- если графическое изображение используется в качестве фона, то текст на этом фоне должен быть хорошо читаем.

Анимация

Анимационные эффекты используются для привлечения внимания слушателей или для демонстрации динамики развития какого-либо процесса. В

этих случаях использование анимации оправдано, но не стоит чрезмерно насыщать презентацию такими эффектами, иначе это вызовет негативную реакцию аудитории.

Звук

- звуковое сопровождение должно отражать суть или подчеркивать особенность темы слайда, презентации;
- необходимо выбрать оптимальную громкость, чтобы звук был слышен всем слушателям, но не был оглушительным;
- если это фоновая музыка, то она должна не отвлекать внимание слушателей и не заглушать слова докладчика. Чтобы все материалы слайда воспринимались целостно, и не возникало диссонанса между отдельными его фрагментами, необходимо учитывать общие правила оформления презентации.

Единое стилевое оформление

- стиль может включать: определенный шрифт (гарнитура и цвет), цвет фона или фоновый рисунок, декоративный элемент небольшого размера и др.;
- не рекомендуется использовать в стилевом оформлении презентации более 3 цветов и более 3 типов шрифта;
- оформление слайда не должно отвлекать внимание слушателей от его содержательной части;
- все слайды презентации должны быть выдержаны в одном стиле;

Содержание и расположение информационных блоков на слайде

- информационных блоков не должно быть слишком много (3-6);
- рекомендуемый размер одного информационного блока — не более 1/2 размера слайда;
- желательно присутствие на странице блоков с разнотипной информацией (текст, графики, диаграммы, таблицы, рисунки), дополняющей друг друга;
- ключевые слова в информационном блоке необходимо выделить;

– информационные блоки лучше располагать горизонтально, связанные по смыслу блоки — слева направо;
– наиболее важную информацию следует поместить в центр слайда;
– логика предъявления информации на слайдах и в презентации должна соответствовать логике ее изложения.

Помимо правильного расположения текстовых блоков, нужно не забывать и об их содержании — тексте. В нем ни в коем случае не должно содержаться орфографических ошибок.

Форма отчетности о результатах самостоятельной работы по дисциплине

- собеседование

- коллоквиум

ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ

Базовый уровень

Тема №1. Принципы функционирования мультиагентных робототехнических систем

Вопросы собеседования:

1. Что такое эмерджентность в мультиагентных системах и как она возникает из локальных правил взаимодействия?

2. В чём различие между централизованной, децентрализованной и иерархической архитектурами МРТС?

Тема №2. Классификация угроз информационной безопасности мультиагентных робототехнических систем

Вопросы собеседования:

1. Какие три основных уровня угроз выделяют в МРТС (физический, коммуникационный, прикладной)? Приведите по одному примеру для каждого.

2. Что такое атака «византийские узлы» и почему она особенно опасна для роевых систем?

Тема №3. Современные методы и модели обеспечения информационной безопасности мультиагентных робототехнических систем

Вопросы собеседования:

1. Как работает модель доверия и репутации для выявления скомпрометированных агентов?

2. Какие криптографические механизмы используются для защиты обмена сообщениями между агентами (MAC, цифровая подпись)?

Тема №4. Методологии и стандарты в области обеспечения информационной безопасности мультиагентных робототехнических систем

Вопросы собеседования:

1. Назовите основной стандарт промышленной кибербезопасности, применимый к МРТС, и его ключевые разделы.

2. Что означает принцип Security by Design при разработке мультиагентных систем?

Повышенный уровень

Тема №1. Принципы функционирования мультиагентных робототехнических систем

Вопросы собеседования:

1. Как наличие гетерогенных агентов (разные ОС, протоколы, производители) влияет на уязвимости системы, и какие архитектурные решения усложняют или упрощают безопасность?

2. Опишите механизм самоорганизации роя на примере алгоритма Boids и укажите, в каком месте злоумышленник может внедрить дезинформацию, чтобы нарушить коллективное движение.

Тема №2. Классификация угроз информационной безопасности мультиагентных робототехнических систем

Вопросы собеседования:

1. В чём отличие «мягкой атаки» (передача дезинформации) от «жёсткой атаки» (физический захват)? Какая из них труднее обнаруживается распределённым IDS?

2. Какая угроза возникает при использовании крупных языковых моделей (LLM) для управления агентами, и как классифицируется эта угроза по модели нарушителя?

Тема №3. Современные методы и модели обеспечения информационной безопасности мультиагентных робототехнических систем

Вопросы собеседования:

1. Как алгоритм византийской отказоустойчивости (PBFT) позволяет достичь консенсуса в рое, если до трети агентов скомпрометированы? Какие накладные расходы это создаёт для ресурсо-ограниченных роботов?

2. Опишите сценарий применения гомоморфного шифрования для агрегации сенсорных данных в МРТС без раскрытия индивидуальных показаний. Какие ограничения существуют у современных гомоморфных схем?

Тема №4. Методологии и стандарты в области обеспечения информационной безопасности мультиагентных робототехнических систем

Вопросы собеседования:

1. Какие требования IEC 62443-3-3 (FR1 – идентификация и аутентификация) наиболее сложно выполнить для роя из 100 дешёвых дронов без аппаратной поддержки TPM? Предложите компромиссные решения.

2. Как можно адаптировать методологию STRIDE для моделирования угроз мультиагентной системы с динамически меняющимся составом агентов? Приведите пример для угрозы подмены (Tampering) данных телеметрии.

1. Критерии оценивания компетенций

Оценка «отлично» выставляется студенту, если

- дополняет свой ответ информацией из дополнительных источников;

- в своей речи использует в полном объеме специальные термины;

- ответ логичен и последователен;

- выводы аргументированы и доказательны.

Оценка «хорошо» выставляется студенту, если

- демонстрирует хорошее владение учебной информацией, определенной рамками учебной дисциплины;

- демонстрирует достаточные знания, владеет специальной терминологией;

- ответ на поставленный вопрос излагается систематизировано и последовательно, при этом допускает определенные неточности в подаче материала.

Оценка «удовлетворительно» выставляется студенту, если

- допускает нарушение в последовательности изложения материала;

- неточно употребляет специальные термины;

- не делает выводы по изложенному материалу (поверхностный характер ответа).

Оценка «неудовлетворительно» выставляется студенту, если

- не последователен, не логичен в ответе;

- не демонстрирует определенные системы знаний по предмету;

- не владеет основной и дополнительной литературой, не делает выводы;

- не владеет понятийным аппаратом по данной дисциплине.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Основная литература:

1. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под редакцией профессора

РАН, доктора технических наук Д.П. Зегжды. – М.: Горячая линия – Телеком, 2020. – 560 с.: ил.

2. Коршунов, Г. И. К70 Сложные киберфизические системы: учеб. пособие / Г. И. Коршунов, И. А. Пастушок, А. А. Петрушевская. – СПб.: ГУАП, 2021. – 141 с.

3. E. A. Lee and S. A. Seshia, Introduction to Embedded Systems - A Cyber-Physical Systems Approach, Second Edition, MIT Press, 2017.

Дополнительная литература:

1. Грибунин В.Г., Мартынов А.П., Николаев Д.Б., Фомченко В.Н. Криптография и безопасность цифровых систем: Учебное пособие / Под ред.

2. Астайкина А.И. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2011, 411 с.

3. Защита информации в компьютерных системах и сетях. / В. Ф. Шаньгин, Москва: ДМК Пресс, 2012. – 592 с.: ил.

4. Информационная безопасность открытых систем [Электронный ресурс]: учебник / Д.А. Мельников. — 3-е изд., стер. — М.: ФлИнта, 2019. — 444 с.

5. Бабаш А.В. Криптографические методы защиты информации. Т. 1: учеб.-метод. пособие / А.В. Бабаш. — 2-е изд. — М.: РИОР: ИНФРА-М, 2018. — 413 с.

6. Криптография и безопасность в технологии .NET /П. Торстейнсон, Г.А. Ганеш; пер.с англ. — 4-е изд., электрон. — М.:Лаборатория знаний, 2020. — 482 с.

Интернет – ресурсы:

1. Официальный сайт Федеральной службы по техническому и экспортному контролю https://fstec.ru/

2. Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) https://rkn.gov.ru/

3. Официальный сайт Федеральной службы безопасности Российской Федерации http://www.fsb.ru/ -

4. Консультант Плюс - законодательство РФ кодексы и законы в последней редакции http://www.consultant.ru/

5. Интернет портал Защита-информации.SU http://www.iso27000.ru/

6. Научная электронная библиотека eLIBRARY.RU http://elibrary.ru

7. Консорциум сетевых электронных библиотек ЭБС «Лань» https://e.lanbook.com/

8. ЭБС «Университетская библиотека ОНЛАЙН» https://www.biblioclub.ru/ -

9. ЭБС IPR SMART https://www.iprbookshop.ru/

10. ЭБС Znanium https://znanium.com/

11. ЭБС «Юрайт» http://www.biblio-online.ru

12. Поисковые интернет-системы Яндекс, Rambler, Google и др.