УТВЕРЖДАЮ

Зав. кафедрой СП ЮУрГУ

\_\_\_\_\_\_\_\_\_Л.Б. Соколинский

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_2022 г.

Фонд оценочных средств

ООП «Инженерия информационных и интеллектуальных систем»

по направлению 09.03.04 – Программная инженерия

Дисциплина «Программирование защищенных интеллектуальных систем»

| **№ КМ** | **Вид КМ** | **Наименование КМ** | **Оценочные средства** |
| --- | --- | --- | --- |
|  | Текущий контроль | Практическая работа № 1 | 1. Перечислите основные виды нормативно-правовых актов, которые существуют на данный момент в мире в области этики искусственного интеллекта.  2. Перечислите и раскройте основные пункты закона о робототехнике России.  3. Перечислите и раскройте основные рекомендации Евросоюза по гражданско-правовым нормам в робототехнике.  4. Перечислите и раскройте основные нормы в законе о робототехнике в США.  5. Перечислите и раскройте основные нормы в законе о робототехнике в Китае.  6. Перечислите и раскройте основные нормы в законе о робототехнике в Канаде. |
|  | Текущий контроль | Практическая работа № 2 | 1. Дайте определение взаимной аутентификации.  2. Имеет ли значение авторизация без аутентификации, и почему.  3. Имеет ли значение авторизация без идентификации, и почему.  4. Имеет ли значение аутентификация без предварительной идентификации, и почему.  5. Имеет ли значение идентификация без аутентификации, и почему.  6. Перечислите и дайте краткую характеристику методам биометрической идентификации. |
|  | Текущий контроль | Практическая работа № 3 | 1. Перечислите требования к используемым алгоритмам искусственного интеллекта в системах информационной безопасности.  2. Каким нормативным документам следует руководствоваться при создании систем искусственного интеллекта, которые работают с персональными данными.  3. Каким нормативным документам следует руководствоваться при создании систем искусственного интеллекта, которые работают с медицинскими данными.  4. Какова роль стандартов информационной безопасности.  5. Перечислите единые критерии безопасности информационных технологий.  6. Пересилите 5 международных стандартов информационной безопасности, и дайте им краткое пояснение. |
|  | Текущий контроль | Практическая работа № 4 | 1. Какие алгоритмы искусственного интеллекта используются для классификации сетевого трафика.  2. Какие алгоритмы искусственного интеллекта используются для сетевых атак.  3. Какие алгоритмы искусственного интеллекта применяют для анализа журналов СЗИ.  4. Перечислите основные правила создания наборов данных для обучения алгоритмов искусственного интеллекта в задаче сетевого трафика.  5. Перечислите методы захвата трафика.  6. Перечислите сетевые анализаторы трафика и принцип их работы. |
|  | Текущий контроль | Практическая работа № 5 | 1. Перечислите основные правила для создания безопасного обучающего набора данных для систем искусственного интеллекта.  2. Перечислите примеры применения искусственного интеллекта в биометрических системах.  3. Перечислите риски при использовании алгоритмов искусственного интеллекта в биометрических системах.  4. Перечислите стандарты создания биометрических систем с использованием алгоритмов искусственного интеллекта.  5. Перечислите алгоритмы искусственного интеллекта для работы с биометрическими данными и приведите примеры.  6. В чем заключается суть биометрической идентификации на основе алгоритмов машинного обучения. |
|  | Текущий контроль | Практическая работа № 6 | 1. Симметричное шифрование.  2. Аутентификация сообщений.  3. Функция хеширования.  4. Дайте определение ключу шифрования.  5. Дайте определение алгоритму шифрования.  6. Как взламывают алгоритмы шифрования? |
|  | Текущий контроль | Тестирование по усвоению материала 1 раздела | 1. Дайте определение искусственного интеллекта.  2. Дайте определение технологии искусственного интеллекта.  3. Перечислите виды искусственного интеллекта.  4. Перечислите формы искусственного интеллекта.  5. Перечислите этапы развития искусственного интеллекта.  6. Перечислите подходы к регулированию искусственного интеллекта. |
|  | Текущий контроль | Тестирование по усвоению материала 2 раздела | 1. Дайте определение этики искусственного интеллекта.  2. Перечислите какой потенциальный вред могут нанести системы искусственного интеллекта.  3. Является ли усложняющим фактором то, что существует множество различных типов искусственного интеллекта.  4. Дайте определение сильному и слабому искусственному интеллекту.  5. Является ли технология искусственного интеллекта этичной или не этичной. |
|  | Текущий контроль | Тестирование по усвоению материала 3 раздела | 1. Перечислите методы статической биометрической идентификации.  2. Дайте определение авторизации.  3. Дайте определение аутентификации.  4. Дайте определение администрированию.  5. Дайте определение идентификации.  6. Перечислите методы идентификации с использованием искусственного интеллекта.  7. Перечислите методы аутентификации с использованием искусственного интеллекта.  8. Перечислите методы администрирования с использованием искусственного интеллекта. |
|  | Текущий контроль | Тестирование по усвоению материала 4 раздела | 1. Как искусственный интеллект помогает в решении задачи анализа возможных угроз.  2. Как искусственный интеллект помогает в решении задачи сетевой безопасности.  3. Как искусственный интеллект помогает в решении задачи моделирования угроз безопасности.  4. Какие существуют правила для формирования доверенного обучающего набора данных.  5. Какие требования должны быть выполнены при проектировании систем искусственного интеллекта. |
|  | Текущий контроль | Тестирование по усвоению материала 5 раздела | 1. Дайте определение вредоносным компьютерным программам.  2. Дайте определение загрузочным вирусам.  3. В чем заключается косвенный способ заражения.  4. Дайте определение макровирусам.  5. В чем заключается суть непосредственного способа размножения.  6. В чем отличия антивирусов с применением алгоритмов искусственного интеллекта.  7. В чем отличия вирусов с применением алгоритмов искусственного интеллекта. |
|  | Текущий контроль | Тестирование по усвоению материала 6 раздела | 1. Перечислите инструменты для интеллектуального анализа данных.  2. Перечислите проблемы искусственного интеллекта в задаче классификации сетевого трафика.  3. Какое влияние на модель оказывает фоновый трафик.  4. Классификация трафика в режиме реального времени.  5. Классификация шифрованного трафика. |
|  | Текущий контроль | Тестирование по усвоению материала 7 раздела | 1. Что может выступать в качестве биометрического идентификатора.  2. На чем основаны динамические методы идентификации.  3. Перечислите динамические методы идентификации.  4. Перечислите статические методы идентификации.  5. На чем основаны статические методы идентификации. |
|  | Текущий контроль | Тестирование по усвоению материала 8 раздела | 1. Дайте определение криптографии.  2. Дайте определение шифрованию.  3. Дайте определение интеллектуальной криптографической системе.  4. Перечислите криптографические технологии обработки данных с использованием технологий искусственного интеллекта.  5. В чем заключается суть механизма безопасной коммуникации на базе алгоритмов искусственного интеллекта. |

Паспорт фонда оценочных средств приведен в п. 6.3 РПД.

Разработчик К.Ю. Никольская

ФГАОУ ВО «Южно-Уральский государственный университет   
(национальный исследовательский университет)»

Кафедра системного программирования

Дисциплина «Программирование защищенных интеллектуальных систем»

ИТОГОВЫЙ ТЕСТ

| № | Вопрос | Варианты ответа |
| --- | --- | --- |
|  | На чем основаны динамические методы идентификации | * поведенческих характеристиках людей * физиологических признаках человека, присутствующих с ним на протяжении всей его жизни |
|  | Перечислите динамические методы идентификации | * идентификация по голосу * идентификация по рукописному почерку * идентификация по клавиатурному почерку * идентификация по лицу |
|  | Перечислите статические методы идентификации | * идентификация по отпечатку пальца * идентификация по термограмме лица * идентификация по рисунку вен * идентификация по клавиатурному почерку * идентификация по голосу |
|  | На чем основаны статические методы идентификации | * физиологических признаках человека, присутствующих с ним на протяжении всей его жизни * поведенческих характеристиках людей |
|  | Является ли технология искусственного интеллекта этичной или не этичной | * да * нет |
|  | Дайте определение авторизации | * процедура распознавания пользователя по его идентификатору (имени). * процедура проверки подлинности заявленного пользователя, процесса или устройства. * процедура предоставления субъекту определенных полномочий и ресурсов в данной системе * регистрация действий пользователя в сети, включая его попытки доступа к ресурсам. |
|  | Дайте определение аутентификации | * процедура распознавания пользователя по его идентификатору (имени). * процедура проверки подлинности заявленного пользователя, процесса или устройства. * процедура предоставления субъекту определенных полномочий и ресурсов в данной системе * регистрация действий пользователя в сети, включая его попытки доступа к ресурсам. |
|  | Дайте определение администрированию | * процедура распознавания пользователя по его идентификатору (имени). * процедура проверки подлинности заявленного пользователя, процесса или устройства. * процедура предоставления субъекту определенных полномочий и ресурсов в данной системе * регистрация действий пользователя в сети, включая его попытки доступа к ресурсам. |
|  | Дайте определение идентификации | * процедура распознавания пользователя по его идентификатору (имени). * процедура проверки подлинности заявленного пользователя, процесса или устройства. * процедура предоставления субъекту определенных полномочий и ресурсов в данной системе * регистрация действий пользователя в сети, включая его попытки доступа к ресурсам. |
|  | Дайте определение взаимной аутентификации | * взаимное подтверждение подлинности субъектов, связывающихся между собой по линиям связи. * одностороннее подтверждение подлинности субъектов, связывающихся между собой по линиям связи. * взаимное подтверждение подлинности субъектов, не связывающихся между собой по линиям связи. |
|  | Имеет ли значение авторизация без аутентификации | * да * нет |
|  | Имеет ли значение авторизация без идентификации | * да * нет |
|  | Имеет ли значение аутентификация без предварительной идентификации | * да * нет |
|  | Имеет ли значение идентификация без аутентификации | * да * нет |
|  | Функция хеширования | * функция, позволяющая создать комбинацию бит, служащую для контроля изменений в зашифрованном сообщении * функция, которая позволяет создать электронную цифровую подпись * функция, позволяющая создать контрольную комбинацию бит, служащую для обнаружения искажений в передаваемом сообщении * функция, которая для строки произвольной длины вычисляет некоторое характерное целое значение или некоторую другую строку фиксированной длины |
|  | Какие алгоритмы искусственного интеллекта используются для сетевых атак | * отравление данных * манипулирование ботами * вирусы |
|  | Для того чтобы прочитать зашифрованную информацию, принимающей стороне необходим: | * ключ * замок * подсказки |
|  | Что такое шифрование? | * способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого * совокупность тем или иным способом структурированных данных и комплексом аппаратно-программных средств * удобная среда для вычисления конечного пользователя |
|  | Что такое криптостойкость? | * характеристика шрифта, определяющая его стойкость к дешифрованию без знания ключа * свойство гаммы * все ответы верны |
|  | Цель криптоанализа: | * Определение стойкости алгоритма * Увеличение количества функций замещения в криптографическом алгоритме * Уменьшение количества функций подстановок в криптографическом алгоритме * Определение использованных перестановок |
|  | Какой слой в структуре системы управления кибербезопасности выделяется в последнее время в качестве отдельного? | * Процессы, персонал * Правила, нормативная база * Данные * Технологии, средства защиты информации |
|  | Какие стадии кибератаки рассматриваются в модели Kill Chain? Выберите все правильные ответы. | * Разведка * Расшифровка * Мониторинг * Реализация * Управление * Прослушивание * Запуск * Анализ |
|  | Какие из перечисленных киберугроз являются ключевыми на ближайшее будущее? Выберите все правильные ответы. | * Устройства IoT как площадка для реализации атак * Спам * Программы-вымогатели * Criminal-as-a-service (переход киберпреступников на сервисную модель) * Программы-шпионы * «Призраки интернета прошлого» * Программы-майнеры * Скимминг |
|  | Что из нижеперечисленного является тенденциями сетевой информационной безопасности? Выберите все правильные ответы. | * Установка накладных средств защиты на сетевые устройства * Интеграция с решениями по расследованию сетевых инцидентов * Инспектирование зашифрованного трафика * Развитие общего сетевого периметра * Интеграция с Threat Intelligence * Уход от использования виртуальных и облачных межсетевых экранов * Мониторинг аномалий во внутренней сети * Внедрение протокола TLS 1.1 для защиты веб-трафика |
|  | Что из нижеперечисленного является тенденциями хостовой информационной безопасности? Выберите все правильные ответы. | * Сдвиг в сторону EDR-решений * Применение узкоспециализированных решений * Использование локальной и облачной песочницы для анализа подозрительных файлов * Обмен данными и командами с решениями по защите сетевых устройств * Избегание SAAS-модели как несущей повышенные риски с точки зрения ИБ * Выбор в пользу единственного корпоративного антивируса и antimalware-движка |
|  | Что из нижеперечисленного является тенденциями Identity & Access Management? Выберите все правильные ответы. | * Более эффективное управление привилегированными пользователями * Внедрение однофакторной аутентификации * Отказ от использования софт-токенов в пользу биометрии * Интеграция со средствами защиты IPS и SIEM * Контроль поведения пользователей с помощью технологии UEBA * Внедрение локальной аутентификации |
|  | Какой способ начала кибератаки самый распространенный в настоящее время? | * Подбор пароля по словарю * Фишинг * Сканирование портов * Перехват сетевого трафика |
|  | В чем особенность кибератак с применением вирусов-шифровальщиков, начиная с 2020? | * Выкуп для расшифрования данных запрашивается неоднократно * Не всегда удается расшифровать данные * Перед шифрованием предпринимается попытка похитить конфиденциальную информацию * Вирус-шифровальщик распространяется по сети, используя незакрытые уязвимости |
|  | Какой тип источников данных относится к слабоструктурированным? Выберите все правильные ответы. | * Базы данных * Потоковые данные (json-сообщения) * XML-файлы * ETL-выгрузки |
|  | Какие компоненты системы аналитического поиска отвечают за доступ пользователей к данным? | * UI + API * Сбор * Хранение * Корреляция |
|  | Какую опасность представляют open-source библиотеки и инструменты в корпоративной среде? Выберите все правильные ответы. | * Часто отсутствуют механизмы аутентификации * Присутствуют избыточные права и повышение привилегий * Используются нестандартные сетевые протоколы * Встречаются незаблокированные стандартные учетные записи * Не допускается сканирование антивирусом * В конфигурационных файлах встречаются пароли в открытом виде |
|  | Продолжите утверждение: главный постулат DATA-DRIVEN состоит в том, что решения нужно принимать, опираясь на… | * Анализ данных, а не интуицию и личный опыт * Результаты анализа AI * Усредненную экспертную оценку * Результаты статистических исследований |
|  | Какая комбинация подходов используется для обнаружения фишинговых сайтов с помощью методов AI? | * CNN + NLP-модели * Logistic Regression + Random Forest * SVM + CNN * NLP-модели + Random Forest |
|  | Какой алгоритм использует AI в антифроде? | * Random forest * Gradient boosting * Isolation forest * Метод k ближайших соседей |
|  | Какой компонент НЕ является моделью машинного обучения в системе контроля конфиденциальной информации? | * Сверточная нейронная сеть * Рекуррентная нейронная сеть * Transformer * Regex-фильтр |
|  | Что служит главным активом для создания решений на основе AI в области кибербезопасности? | * Структурированные данные * Цифровые следы всех процессов * Потоковая информация в реальном времени * Алгоритмы |
|  | Какая технология AI позволила совершить качественный прорыв в обработке текстов? | * Bag of words * TF-IDF * Transformers * Logistic Regression |
|  | Каков уровень зрелости open-source инструментов ML в антифроде? | * Позволяют “из коробки” решать сложные практические задачи * Можно использовать в масштабных задачах, но требуется существенная доработка * Подходят для решения только простых задач * Применяются только как компонент в коммерческих решениях |
|  | Какую модель рекомендуется использовать при реагировании на инциденты кибербезопасности? | * ITIL * COBIT * Cyber Kill-Chain * TIP |
|  | Что НЕ входит в функционал подразделений кибербезопасности? | * Обнаружение уязвимостей * Оценка критичности * Устранение уязвимостей * Подготовка отчетности по киберугрозам |