Вопросы к экзамену по модулю «Методы классификации из ML в ИБ»

|  |  |
| --- | --- |
| № | Вопрос |
| 1 | Выберите наиболее правильное определение «вредоносное программное обеспечение»:   1. Любое программное обеспечение, предназначенное для санкционированного доступа к вычислительным ресурсам ЭВМ или к информации, хранящейся на ЭВМ. 2. Системное программное обеспечение, предназначенное для несанкционированного доступа к вычислительным ресурсам ЭВМ или к информации, хранящейся на ЭВМ,. 3. **Любое программное обеспечение, предназначенное для несанкционированного доступа к вычислительным ресурсам ЭВМ или к информации, хранящейся на ЭВМ.** 4. Прикладное программное обеспечение, предназначенное для несанкционированного доступа к вычислительным ресурсам ЭВМ или к информации, хранящейся на ЭВМ, |
| 2 | Большинство вредоносных программ:   1. Предоставляют доступ к своему исходному коду 2. **Отлавливаются в ловушках-песочницах** 3. Блокируются Интернет-провайдерами 4. Возможно обнаружит и обезвредить рядовому пользователю |
| 3 | Выберите операционную систему, под которую невозможно создать вредоносное ПО   1. Windows 2. Mac 3. Linux 4. **Все варианты не верны** |
| 4 | Conficker —это   1. **Семейство червей, нацеленных на ОС Windows** 2. Семейство троянов, нацеленных на ОС Android 3. Антивирус 4. Дистрибутив Linux для поиска уязвимотей |
| 5 | Преимущество метода сигнатур перед методами машинного обучения:   1. Нечёткое сравнение 2. Адаптируемость 3. **Меньшее количество ложных срабатываний** 4. Устойчивость к изменению кода вредоносного ПО |
| 6 | Что не является общим типом поведения вредоносного ПО   1. Маскировка присутствия 2. Стремление к выполнению своей функции 3. Сбор данных 4. **Адаптируемость** |
| 7 | Выберите динамические методы генерации признаков   1. **Анализ поведение** 2. Анализ структуры 3. **Отладка** 4. Метод сигнатур |
| 8 | Выберите качества, присущие Q-learning:   1. Может работать с непрерывными действиями 2. **Может обучаться на исторических данных** 3. Принимает решение об оптимальном действии на каждом шаге 4. **Оценивает размер возможной награды для каждого действия** |
| 9 | Выберите методы неявного представления признаков:   1. **SVD** 2. ANOVA 3. **PCA** 4. RFE |
| 10 | Выберите методы глубокого обучения без учителя:   1. CNN 2. **Autoencoder** 3. **Policy gradient** 4. SGD |