Университет ИТМО, факультет инфокоммуникационных технологий Отчетная работа по «Информатике»: аннотация к статье

Выполнила Касьяненко В.М., № группы К3121, дата 19.11.2022, оценка ФИО студента не заполнять

Название статьи/главы книги: Машинное обучение в кибербезопасности		
ФИО автора статьи: Боброва М.В., Мастилин А.Е.	**Дата публикации:** 2021 г.	**Размер статьи** 6 стр.
Прямая полная ссылка на источник и сокращенная ссылка: https://cyberleninka.ru/article/n/mashinnoe-obuchenie-v-kiberbezopasnosti https://goo.su/rhB2r		
Тэги, ключевые слова или словосочетания кибербезопасность / машинное обучение / МО / кибератаки		
Перечень фактов, упомянутых в статье: Кибербезопасность является одной из главных проблем современного мира. Одним из способов решения этой проблемы является использование машинного обучения (МО). Машинное обучение – метод, при помощи которого машины учатся делать логические выводы и прогнозировать результаты на основе каких-либо данных. Существует несколько видов обучения машин: контролируемое, неконтролируемое и обучение с подкреплением. При контролируемом обучении машина использует размеченные данные с правильными ответами, с которыми сравнивает полученные результаты, тем самым обучаясь, а при неконтролируемом обучении машина самостоятельно выявляет шаблоны во входных данных. Обучение с подкреплением использует систему вознаграждения за правильные ответы, что позволяет получить наилучший результат при анализе данных. Машинное обучение в кибербезопасности может применяться для решения широкого круга задач, например для выявления необычного поведения, уязвимостей в системе и их исправления. Некоторые крупные компании, такие как Лаборатория Касперского, используют машинное обучение для предотвращения кибератак, распространения защитных мер и идентификации разработчиков вредоносных программ. Однако данная технология не может обеспечить полную безопасность систем, поскольку при ее использовании невозможно учесть все нюансы, которые могут возникнуть при определенных условиях.		
Позитивные следствия и/или достоинства описанной в статье технологии - множество вариантов использования - автоматизация обнаружения кибератак - технология значительно сокращает время обнаружения подозрительного поведения		
Негативные следствия и/или недостатки описанной в статье технологии - не может обеспечить полную безопасность - может нарушать законы из-за использования конфиденциальной информации - недостаточное количество данных может привести к неправильным решениям		
Ваши замечания, пожелания преподавателю или анекдот о программистах		