стояние). В проекте инициализация состояний происходит при создании объекта бота.

ЛИТЕРАТУРА

1. Руководство по программированию на C# [Электронный ресурс] – Режим доступа: https://learn.microsoft.com/ru-ru/dotnet/csharp/programming-guide – Дата доступа: 29.03.2024.

2. Официальная документация Unity [Электронный ресурс] – Режим доступа: https://docs.unity.com – Дата доступа: 08.04.2023.

3. Официальная документация GitHub [Электронный ресурс]. Режим доступа: https://docs.github.com. Дата доступа: 11.04.2024.

УДК 004.62

Студ. А.М. Жук
Науч. рук. ассист. О.А. Нистюк
(Кафедра информационных систем и технологий, БГТУ)

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ХРАНЕНИЯ ИСПОЛЬЗУЕМЫХ В МАШИННОМ ОБУЧЕНИИ ДАННЫХ

Обеспечение безопасности данных, используемых в процессе машинного обучения, является критически важной задачей. Данные, используемые для обучения моделей, могут содержать конфиденциальную информацию, которую необходимо защищать.

На практике данные хранятся в базах данных, которые могут быть размещены на физических серверах или в облаке. Физические серверы обеспечивают полный контроль над данными и их безопасностью. Но они также требуют значительных затрат. Облачные серверы, с другой стороны, предлагают гибкость и масштабируемость, с другой – могут представлять риски для безопасности.

Особое внимание следует уделить анонимизации данных. Этот процесс позволяет скрыть идентифицирующие атрибуты. Очень важно проводить анонимизацию данных уже на этапе сбора и подготовки, сделать это можно с помощью маскирования [1], которое представляет собой процесс скрытия чувствительных атрибутов данных путем замены их на заглушки или маски.

Если не анонимные данные уже попали в руки инженера машинного обучения, важно применить процедуры псевдонимизации [2] и шифрования данных. Первая позволяет заменить идентифицирующую информацию на искусственные идентификаторы или псевдонимы. Шифрование преобразует данные в форму, которую можно прочитать только с использованием специального ключа, что обеспечивает дополнительный уровень защиты, предотвращая несанкциониро-

ванный доступ к данным даже в случае их утечки. При завершении обучения модели можно использовать обфускацию [3], то есть приведения исходного кода программы к виду, сохраняющему исходную функциональность, но затрудняющему анализ, понимание алгоритмов работы и модификацию при декомпиляции. Обеспечение безопасности данных в процессе машинного обучения требует комплексного подхода, включающего в себя безопасное хранение данных, контроль доступа и анонимизацию данных.

ЛИТЕРАТУРА

1. Маскировка данных [Электронный ресурс]. – Режим доступа: https://aws.amazon.com/ru/what-is/data-masking/ – Дата доступа: 20.03.2024.

2. Псевдонимизация как инструмент безопасности и способ легитимной обработки персональных данных. [Электронный ресурс]. – Режим доступа: https://ib-bank.ru/bisjournal/news/13533 – Дата доступа: 20.03.2024.

3. Обфускация кода – что, как и зачем [Электронный ресурс]. – Режим доступа: https://habr.com/ru/articles/735812/. – Дата доступа: 20.03.2024.

УДК 004.4

Студ. Д.М. Пирейко
Науч. рук. ассист. П.В. Бернацкий
(кафедра информационных систем и технологий, БГТУ)

ОСВЕДОМЛЕННОСТЬ ПОЛЬЗОВАТЕЛЯ И СРЕДСТВА ЕЕ ДОСТИЖЕНИЯ В СИСТЕМАХ КОНТРОЛЯ УПРАВЛЕНИЯ РАЗРАБОТКОЙ IT-ПРОДУКТА

Осведомленность пользователя является важным аспектом в разработке IT-продуктов. Чтобы обеспечить высокую осведомленность пользователей, следует использовать различные средства в системах контроля управления разработкой (СКУР). Вот несколько способов достижения осведомленности пользователей в СКУР:

1. Документация и руководства: Создание подробной документации и руководств, которые описывают функциональность и использование продукта, может помочь пользователям лучше понять, как работает IT-продукт.

2. Обратная связь и коммуникация: Взаимодействие с пользователями позволяет получить обратную связь от них, а также предоставить им информацию о новых функциях, исправлениях ошибок и других изменениях в продукте [1].