

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

Кафедра технологий программирования

ИДЕИ В ОБЛАСТИ «БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ»

Домашнее задание

Шибко Татьяны Александровны
студентки 4 курса 12 группы
специальность "прикладная информатика"

Дата окончания работы 29.09.2024 г.

Преподаватель:
Доцент К.А. Зубович

Минск, 2024

1. ВЫДЕЛЯЕМ ОБЩЕЕ ИЗ 10 ЗАМЕТОК В ЛЕКЦИИ

Сначала давайте посмотрим на то, какие заметки у нас есть.

Набрал «Безопасность информационных систем» и «попросил» сформулировать 10 идей. Получил:

1. Разработка программного обеспечения с встроенными защитными механизмами, которые автоматически обнаруживают и блокируют попытки взлома или несанкционированного доступа к системе.
2. Создание специального программного обеспечения, которое может обнаруживать и отслеживать попытки вирусов, шпионских программ и других вредоносных программ, которые могут инфицировать системы.
3. Разработка алгоритмов искусственного интеллекта, которые могут анализировать поведение пользователей и выявлять подозрительные действия, такие как частые посещения запрещенных сайтов или использование недопустимых приложений.
4. Создание систем, которые могут обнаруживать и удалять вредоносное ПО автоматически, без необходимости вмешательства пользователя.
5. Разработка системы, которая автоматически обнаруживает и блокирует попытки взлома системы, используя технологии машинного обучения и искусственного интеллекта.
6. Создание системы, которая может анализировать и идентифицировать случаи кражи данных или несанкционированного доступа, чтобы предотвратить утечку конфиденциальной информации.
7. Разработка специальных устройств, которые могут защитить компьютер или другое электронное устройство от взлома через вибрацию или звуковые волны.
8. Создание системы, которая может обнаружить и предотвратить попытки несанкционированного доступа к информации, используя технологии распознавания голоса и лица.
9. Разработка системы, которая может обнаруживать и блокировать попытки атаки на компьютерную сеть, используя системы анализа трафика и сетевых устройств.
10. Создание системы, которая может анализировать и определять причины утечки информации, например, через слабый пароль или ненадежную защиту от хакерских атак

Набрал «Безопасность инфосистем» получил :

1. Разработка системы антивирусов на базе искусственного интеллекта, которая будет постоянно анализировать и обнаруживать новые угрозы.
2. Создание облачной платформы, которая будет предоставлять пользователям мгновенную защиту от хакерских атак.
3. Разработка алгоритмов машинного обучения, которые будут автоматически обнаруживать уязвимости в инфосистемах и исправлять их до того, как они приведут к серьезным последствиям.
4. Создание системы автоматического резервного копирования данных, которая будет создавать резервные копии инфосистем в случае отказа оборудования или других технических проблем.
5. Разработка программного обеспечения, которое позволит пользователям создавать и управлять своими собственными инфосистемами, используя только один интерфейс.
6. Создание системы мониторинга, которая будет отслеживать и предупреждать о любых потенциальных угрозах безопасности инфосистем, позволяя быстро реагировать на них.
7. Разработка системы обнаружения вторжений на уровне ядра операционной системы, которая будет реагировать на любые попытки проникновения в инфосистемы и оповещать пользователей о возможных угрозах.
8. Создание системы защиты от физического взлома, которая будет обеспечивать защиту от несанкционированного доступа к инфосистемам.
9. Разработка технологии, которая позволит управлять и контролировать все компоненты инфосистем, что позволит устранить любые уязвимости и обеспечить максимальную безопасность данных.
10. Создание системы обнаружения и предотвращения кибератак на основе блокчейн-технологии, которая будет обеспечивать защиту и безопасность инфосистем от мошенничества и хакерских атак.

После подробного изучения, можно выделить следующие пересечения (или общие моменты). Просьба не ругаться на плохие слова, я цитировала:

1. Заметка 1, пункт 1: Разработка программного обеспечения с встроенными защитными механизмами, которые автоматически обнаруживают и блокируют попытки взлома или несанкционированного доступа к системе.

Заметка 2, пункт 7: Разработка системы обнаружения вторжений на уровне ядра операционной системы, которая будет реагировать на любые попытки

проникновения в инфосистемы и оповещать пользователей о возможных угрозах.

2. Заметка 1, пункт 2: Создание систем, которые могут обнаруживать и удалять вредоносное ПО автоматически, без необходимости вмешательства пользователя.

Заметка 2, пункт 1: Разработка системы антивирусов на базе искусственного интеллекта, которая будет постоянно анализировать и обнаруживать новые угрозы.

3. Заметка 1, пункт 3: Разработка алгоритмов искусственного интеллекта, которые могут анализировать поведение пользователей и выявлять подозрительные действия.

Заметка 2, пункт 3: Разработка алгоритмов машинного обучения, которые будут автоматически обнаруживать уязвимости в инфосистемах и исправлять их до того, как они приведут к серьезным последствиям.

4. Заметка 1, пункт 4: Создание системы автоматического резервного копирования данных, которая будет создавать резервные копии инфосистем в случае отказа оборудования или других технических проблем.

Заметка 2, пункт 4: Создание системы автоматического резервного копирования данных, которая будет создавать резервные копии инфосистем в случае отказа оборудования или других технических проблем.

5. Заметка 1, пункт 5: Создание системы мониторинга, которая будет отслеживать и предупреждать о любых потенциальных угрозах безопасности инфосистем.

Заметка 2, пункт 6: Создание системы мониторинга, которая будет отслеживать и предупреждать о любых потенциальных угрозах безопасности инфосистем, позволяя быстро реагировать на них. (Сходство в сути, но акценты разные)

6. Заметка 1, пункт 6: Создание системы, которая может обнаружить и предотвратить попытки несанкционированного доступа к информации, используя технологии распознавания голоса и лица.

Заметка 2, пункт 8: Создание системы защиты от физического взлома, которая будет обеспечивать защиту от несанкционированного доступа к инфосистемам. (Сходство в идее защиты доступа, но разные подходы)

Теперь попробуем объединить оба множества.

1. Разработка системы антивирусов на базе искусственного интеллекта, которая будет постоянно анализировать и обнаруживать новые угрозы.

2. Создание системы, которая может анализировать и идентифицировать случаи кражи данных или несанкционированного доступа, чтобы предотвратить утечку конфиденциальной информации.
3. Создание системы, которая может обнаружить и предотвратить попытки несанкционированного доступа к информации, используя технологии распознавания голоса и лица.
4. Разработка алгоритмов машинного обучения, которые будут автоматически обнаруживать уязвимости в инфосистемах и исправлять их до того, как они приведут к серьезным последствиям.
5. Создание системы мониторинга, которая будет отслеживать и предупреждать о любых потенциальных угрозах безопасности инфосистем, позволяя быстро реагировать на них.

Что касается пояснений «а почему так», то могу предположить следующее:

1. Фокус на специфике:

Запрос «Безопасность информационных систем» может подразумевать более широкий и общий подход к безопасности, охватывающий различные аспекты и технологии. В то же время, другой запрос («Безопасность инфосистем») может акцентировать внимание на более узких, технических решениях, связанных с конкретными системами и их защитой.

2. Тренды и технологии:

Разные наборы запросов могут отражать текущие тренды (то, что популярно или широко используется в данный момент времени... ну или по последнему обучению модели) в области информационной безопасности. Например, упоминание облачных технологий и блокчейна может быть более актуальным в одном контексте, чем в другом.

3. Целевая аудитория:

Разные запросы могут ориентироваться на разные группы пользователей (например, разработчиков, администраторов или простых работяг, то есть обычных пользователей), что влияет на формулировку идей.

2. ОПРЕДЕЛЕНИЕ НЕЦЕНЗУРНОЙ БРАНИ

Набрал «Безопасность информационных систем» и «попросил» сформулировать 10 идей. Получил:

1. Разработка программного обеспечения с встроенными защитными механизмами, которые автоматически обнаруживают и блокируют попытки взлома или несанкционированного доступа к системе. 2. Создание специального программного обеспечения, которое может обнаруживать и отслеживать

попытки вирусов, шпионских программ и других вредоносных программ, которые могут инфицировать системы. 3. Разработка алгоритмов **искусственного интеллекта**, которые могут анализировать поведение пользователей и выявлять подозрительные действия, такие как частые посещения запрещенных сайтов или использование недопустимых приложений. 4. Создание систем, которые могут обнаруживать и удалять вредоносное **ПО** автоматически, без необходимости вмешательства пользователя. 5. Разработка системы, которая автоматически обнаруживает и блокирует попытки взлома системы, используя технологии машинного обучения и **искусственного интеллекта**. 6. Создание системы, которая может анализировать и идентифицировать случаи кражи данных или несанкционированного доступа, чтобы предотвратить утечку конфиденциальной информации. 7. Разработка специальных устройств, которые могут защитить компьютер или другое электронное устройство от взлома через вибрацию или звуковые волны. 8. Создание системы, которая может обнаружить и предотвратить попытки несанкционированного доступа к информации, используя технологии распознавания голоса и лица. 9. Разработка системы, которая может обнаруживать и блокировать попытки атаки на компьютерную сеть, используя системы анализа трафика и сетевых устройств. 10. Создание системы, которая может анализировать и определять причины утечки информации, например, через слабый пароль или ненадежную защиту от хакерских атак

Набрал «Безопасность инфосистем» получил :

1. Разработка системы **антивирусов** на базе **искусственного интеллекта**, которая будет постоянно анализировать и обнаруживать новые угрозы.
2. Создание **облачной платформы**, которая будет предоставлять пользователям мгновенную защиту от хакерских атак.
3. **Разработка алгоритмов машинного обучения**, которые будут автоматически обнаруживать уязвимости в **инфосистемах** и исправлять их до того, как они приведут к серьезным последствиям.
4. Создание системы автоматического резервного копирования данных, которая будет создавать резервные копии **инфосистем** в случае отказа оборудования или других технических проблем.
5. **Разработка программного обеспечения**, которое позволит пользователям создавать и управлять своими собственными **инфосистемами**, используя только один интерфейс.
6. Создание **системы мониторинга**, которая будет отслеживать и предупреждать о любых потенциальных угрозах безопасности **инфосистем**, позволяя быстро реагировать на них.
7. Разработка системы обнаружения вторжений на уровне ядра операционной системы, которая будет реагировать на любые попытки проникновения в **инфосистемы** и оповещать пользователей о возможных угрозах.
8. Создание системы защиты от физического взлома, которая будет обеспечивать защиту от несанкционированного доступа к **инфосистемам**.
9. Разработка технологии, которая позволит управлять и контролировать все компоненты **инфосистем**, что позволит устранить любые уязвимости и обеспечить максимальную безопасность данных.
10. Создание системы обнаружения и предотвращения **кибератак** на основе **блокчейн-технологии**, которая будет обеспечивать защиту и безопасность **инфосистем** от мошенничества и хакерских атак.