МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ   
РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение

высшего образования

«Российский государственный университет им. А.Н. Косыгина   
(Технологии. Дизайн. Искусство)»

Отчет по лабораторной работе № 5

по дисциплине «Информационные и коммуникационные

технологии в профессиональной деятельности»

Тема: «Работа с нейросетями»

Выполнил: Ольховский Н.С.

Проверила: Вахромеева Е.Н.

Москва 2024

**Задание 1**

**Наименование нейросети**: GigaChat

**Простой запрос**: Напиши текст объемом 20-25 предложений на тему "Риски и угрозы информационной безопасности в мобильных приложениях".

**Полученный текст**: В современном мире мобильные приложения стали неотъемлемой частью повседневной жизни миллионов людей по всему миру. Они предоставляют удобство, скорость и доступ к различным сервисам прямо с экрана смартфона. Однако вместе с этим растут риски и угрозы для информационной безопасности пользователей.

Одной из основных угроз является утечка данных. Мобильные устройства часто содержат конфиденциальную информацию – от личных контактов до банковских реквизитов. Приложения могут собирать эти данные без ведома пользователя и передавать их третьим лицам, что создает риск несанкционированного доступа к личной информации.

Еще одной серьезной угрозой являются уязвимости программного обеспечения. Ошибки в коде приложений могут быть использованы злоумышленниками для проведения атак, таких как внедрение вредоносного кода или кража данных. Регулярные обновления и патчи помогают снизить этот риск, но не все пользователи устанавливают их вовремя.

Фишинговые атаки также представляют значительную угрозу. Злоумышленники создают поддельные версии популярных приложений, которые выглядят как настоящие, но на самом деле предназначены для кражи учетных данных или установки вредоносного ПО. Пользователи должны быть осторожны при загрузке приложений только из официальных магазинов и проверять отзывы перед установкой.

Мошеннические схемы через мобильные приложения становятся все более распространенными. Например, злоумышленники могут создавать фальшивые приложения для оплаты услуг, которые вместо этого крадут деньги у пользователей. Важно внимательно читать условия использования и избегать подозрительных приложений.

Кроме того, существует угроза перехвата данных во время передачи между устройством и сервером. Если приложение не использует шифрование, то информация может быть легко перехвачена и использована злоумышленниками. Поэтому важно выбирать приложения, которые обеспечивают высокий уровень защиты данных.

Также стоит отметить проблему сторонних библиотек и SDK (Software Development Kit), которые разработчики используют для ускорения процесса создания приложений. Эти компоненты могут содержать уязвимости, о которых сами разработчики могут не знать. Это делает приложения потенциально опасными даже если они кажутся безопасными.

Наконец, нельзя забывать о рисках, связанных с использованием публичных Wi-Fi сетей. При подключении к таким сетям данные могут быть перехвачены злоумышленниками, поэтому рекомендуется использовать VPN-сервисы для дополнительной защиты.

Таким образом, информационная безопасность в мобильных приложениях требует особого внимания со стороны как разработчиков, так и пользователей. Необходимо регулярно обновлять программное обеспечение, тщательно выбирать приложения и следить за своими действиями в сети. Только комплексный подход позволит минимизировать риски и обеспечить защиту персональных данных.

**Запрос инструкция**: Напиши текст объемом 20-25 предложений на тему "Риски и угрозы информационной безопасности в мобильных приложениях". В тексте должна быть информация о Man In The Middle attack, а также несколько примеров известных типов атак.

**Полученный текст**: Современные мобильные приложения играют важную роль в нашей повседневной жизни, предоставляя удобный доступ к разнообразным услугам и функциям. Однако, несмотря на все преимущества, использование этих приложений связано с рядом рисков и угроз для информационной безопасности. Одной из наиболее опасных атак является Man-in-the-Middle (MITM) атака, которая позволяет злоумышленнику перехватывать и изменять данные, передаваемые между пользователем и сервером.

Man-in-the-Middle атака заключается в том, что злоумышленник вставляется между двумя сторонами коммуникации, незаметно подменяя себя одним из участников обмена данными. Например, пользователь мобильного приложения может считать, что он общается напрямую с сервером, тогда как на самом деле его сообщения проходят через посредника, который может просматривать, модифицировать или удалять информацию. MITM-атаки особенно опасны, когда используются публичные Wi-Fi-сети, где защита трафика может быть минимальной.

Другой тип атаки — это фишинг, при котором злоумышленники создают поддельные сайты или приложения, имитирующие легитимные сервисы, чтобы обмануть пользователей и заставить их ввести свои личные данные, такие как логины и пароли. Примером такой атаки может служить создание фейкового банковского приложения, которое выглядит идентично оригинальному, но собирает введенные пользователями данные для последующего мошенничества.

SQL-инъекции — еще одна известная угроза, связанная с мобильными приложениями. Эта атака направлена на базы данных, использующие SQL-запросы. Злоумышленник вводит специально сформированные запросы, которые позволяют ему получить доступ к данным или изменить их. Такая атака может привести к утечке чувствительной информации, например, номеров кредитных карт или другой финансовой информации.

Переполнение буфера — классическая атака на программные системы, включая мобильные приложения. Она происходит, когда злоумышленник отправляет больше данных, чем приложение ожидает обработать, что приводит к переполнению памяти и выполнению произвольного кода. Это может дать хакеру контроль над устройством жертвы.

Не менее важной проблемой является утечка данных. Многие мобильные приложения собирают большое количество персональной информации, такую как местоположение, контакты, историю браузера и т.д., что делает их привлекательными целями для киберпреступников. Если приложение недостаточно защищено, эта информация может попасть в руки злоумышленников, что приведет к серьезным последствиям для пользователей.

Эти примеры показывают, насколько важно уделять внимание вопросам информационной безопасности при разработке и использовании мобильных приложений. Разработчики должны применять современные методы защиты, такие как шифрование данных, аутентификация пользователей и регулярные обновления безопасности. Пользователи же должны быть внимательны при установке приложений, избегать ненадежных источников и всегда использовать защищенное соединение при передаче важных данных.

**Задание 2**

**Наименование нейросети**: ChatGPT

**Простой запрос**: Напиши текст объемом 20-25 предложений на тему "Риски и угрозы информационной безопасности в мобильных приложениях".

**Полученный текст**: С распространением мобильных технологий и увеличением числа пользователей смартфонов, вопросы информационной безопасности становятся особенно актуальными. Мобильные приложения, используемые для различных целей, представляют собой потенциальные мишени для злоумышленников. Одним из основных рисков является несанкционированный доступ к личным данным пользователей, таким как контакты, фотографии и геолокация. Часто разработчики не уделяют должного внимания защите данных, что делает приложения уязвимыми для атак.

Еще одним значительным риском является распространение вредоносного ПО через мобильные приложения. Злоумышленники могут создавать поддельные приложения, которые выглядят как легитимные, но на самом деле направлены на кражу информации. Такие приложения часто размещаются в сторонних магазинах, что затрудняет их обнаружение обычными пользователями. Вдобавок, использование публичных Wi-Fi сетей увеличивает вероятность перехвата данных, передаваемых между устройством и сервером.

Также следует упомянуть о рисках, связанных с недостаточной защитой данных при их использовании в облачных сервисах. Пользователи могут не осознавать, что их информация хранится на удаленных серверах, что создает дополнительные уязвимости. Шифрование данных является одним из способов защиты, однако многие приложения не реализуют эту функцию должным образом.

Наконец, человеческий фактор также играет важную роль в сфере безопасности. Невнимательность пользователей, которые устанавливают небезопасные приложения или используют простые пароли, может привести к компрометации аккаунтов. Важно, чтобы разработчики и компании, занимающиеся мобильными приложениями, проводили регулярные аудиты безопасности и информировали пользователей о лучших практиках защиты. Принятие мер по обеспечению безопасности на каждом этапе разработки и эксплуатации приложений может существенно снизить риски и угрозы информационной безопасности.

**Запрос инструкция**: Напиши текст объемом 20-25 предложений на тему "Риски и угрозы информационной безопасности в мобильных приложениях". В тексте должна быть информация о Man In The Middle attack, а также несколько примеров известных типов атак.

**Полученный текст**: С ростом использования мобильных приложений растет и количество угроз информационной безопасности, с которыми сталкиваются пользователи. Одной из наиболее распространенных атак является атака "Человек посередине" (Man In The Middle, MITM). В ходе этой атаки злоумышленник может перехватывать и изменять данные, передаваемые между устройством пользователя и сервером. Например, если пользователь подключается к общественной Wi-Fi сети, злоумышленник может создать точку доступа с похожим именем и обманом заставить пользователя подключиться к ней. Это открывает возможности для перехвата личной информации, таких как пароли и финансовые данные.

Кроме MITM, существует множество других типов атак, угрожающих мобильным приложениям. Атаки на основе подмены DNS позволяют мошенникам перенаправлять трафик на фальшивые веб-сайты, где пользователи могут вводить свои учетные данные. Вредоносные приложения могут содержать трояны, которые крадут информацию или дают злоумышленнику полный контроль над устройством. Также стоит упомянуть фишинг, когда пользователи получают сообщения с просьбой перейти по ссылке и ввести свои данные на фальшивых страницах.

Некоторые приложения сохраняют данные в незащищенном виде, что делает их уязвимыми для прямого доступа при наличии физического доступа к устройству. Нередко пользователи устанавливают приложения из непроверенных источников, что также увеличивает риск заражения вредоносным программным обеспечением. Неправильные настройки безопасности, такие как отсутствие шифрования, могут привести к утечке личной информации.

Несмотря на множество угроз, пользователи могут минимизировать риски, соблюдая основные правила безопасности, такие как использование сложных паролей и двухфакторной аутентификации. Разработчики в свою очередь должны уделять внимание защите данных, внедряя современные решения для шифрования и регулярно тестируя приложения на наличие уязвимостей. Сложность информационной безопасности становится все более заметной, и важно, чтобы как пользователи, так и разработчики принимали активные меры для защиты своих данных.

**Задание 3**

**Облака слов**

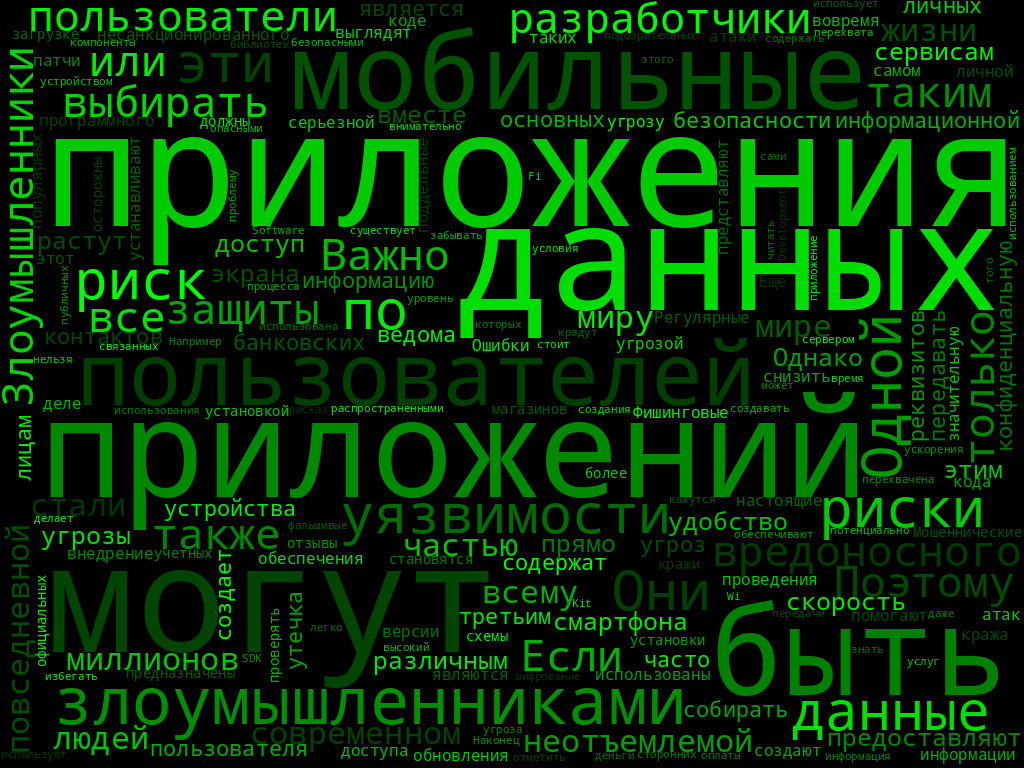


Рис. 1. Простой запрос задание 1

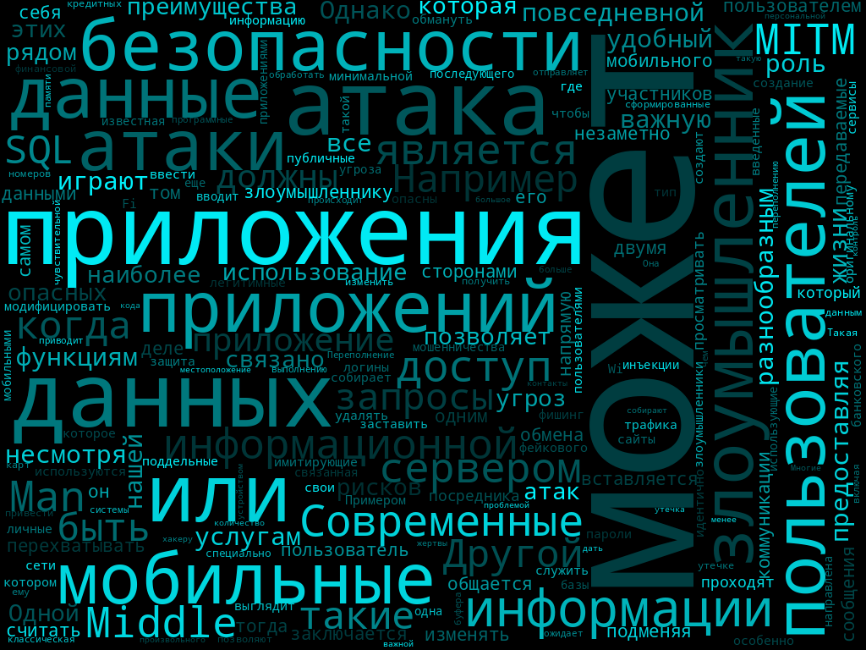


Рис. 2. Запрос инструкция задание 1

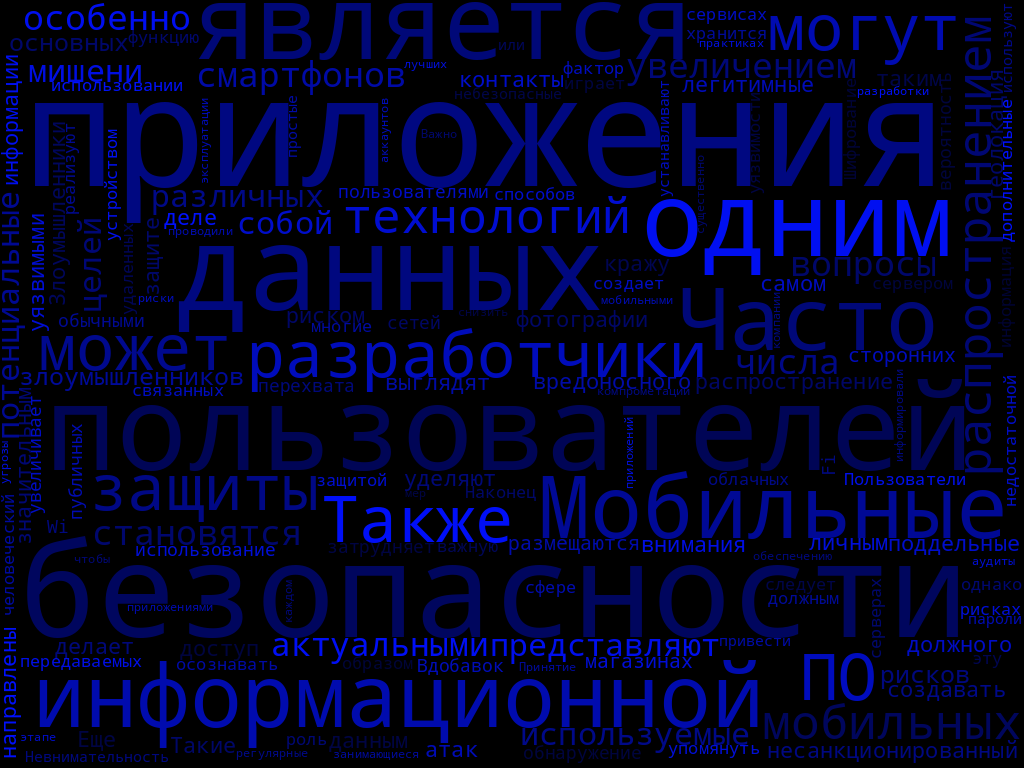


Рис. 3 Простой запрос задание 2

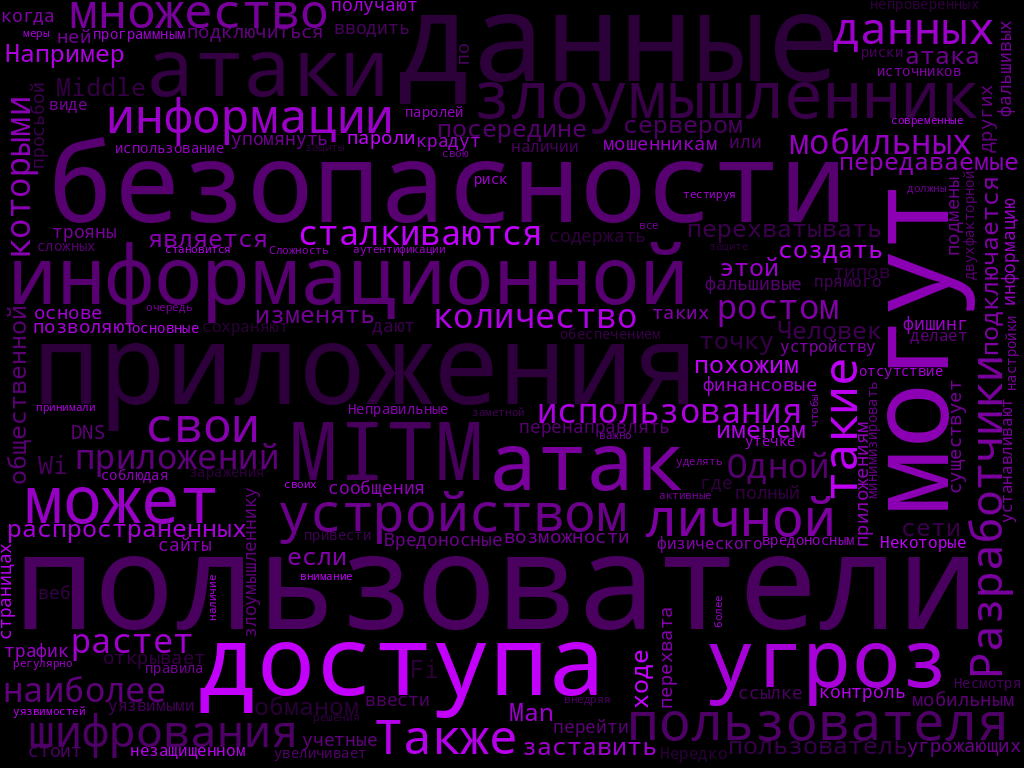


Рис. 4. Запрос инструкция задание 2

**Задание 4**

**Сходства/различия:** Обе нейросети сгенерировали похожие по структуре тексты: вступление, разбор ключевых идей, заключение. Схожими оказались вступление и заключение. В основном тексте GigaChat выделяет конкретные виды угроз и коротко описывает каждую. ChatGPT выделяет общие причины угроз, описывает их, не вдаваясь в конкретные детали.

**Признаки сгенерированного текста**:

Повторяющийся вид предложений: В основном тексте каждый абзац имеет вид термин – пояснение. Встречаются похожие предложения и словосочетания. Обе нейросети не включили в текст примеры.

**Обнаруженные неточности/недочеты**:

ChatGPT сгенерировал всего по 15 предложений для каждого текста вместо необходимых 20. У ChatGPT отсутствует выделенное заключение.

**Личное впечатление**: GigaChat описал конкретные виды угроз, что не даёт общего понимания, почему такие угрозы возникают. ChatGPT на мой взгляд более корректно выполнил задание, описав основные темы проблемы.

**Задание 5**

**Нейросеть:** Artguru

**Запрос**: Нарисуй хакера мобильных приложений.



Рис. 4. Запрос задание 5.

**Задание 6**

1. **Недочеты в иллюстрации**

Нейросеть имеет проблему с генерацией рук, в особенности пальцев.

Телефон непонятного размера.

Задний фон нереалистичен.

На столе лежат непонятная канцелярия.

1. **Ожидаемые/фактический результат**

Ожидалось увидеть более реалистичное изображение, где хакер — это обычный человек с одним телефоном, подключённым к компьютеру, а не мобильного геймера.

1. **Личное впечатление**

Нейросеть плохо справилась со своей задачей, она отстает от современных тенденций, качество картинки не соответствует необходимым требованиям, хотя в целом может быть использовано.

**Задание 7**

**Запрос:** Напиши краткий план для данной презентации

**Результат:**

1. **Введение**
   * Определение кибератак.
   * Примеры угроз: фишинг, DDoS-атаки, вредоносные программы.
2. **Основные методы защиты**
   * Антивирусные программы.
   * Межсетевые экраны.
   * Шифрование данных.
   * Обновление программного обеспечения.
3. **Современные технологии противодействия**
   * Системы обнаружения и предотвращения вторжений (IDS/IPS).
   * Искусственный интеллект и машинное обучение.
   * Использование блокчейна.
4. **Важность комплексного подхода**
   * Комбинирование технологий.
   * Обучение сотрудников.
   * Регулярный аудит безопасности.
5. **Современные вызовы и решения**
   * Эволюция атак с использованием ИИ.
   * Атаки на облачные сервисы и IoT.
   * Укрепление законодательства и международное сотрудничество.
6. **Заключение**
   * Поддержание актуальности технологий защиты.
   * Комплексный подход для устойчивости инфраструктур.

Такой план поможет структурировать презентацию и выделить ключевые моменты.

**Задание 8**

**Запрос**: Напиши краткий план для презентации на тему “Технологии и методы защиты от вредоносных программ”. Презентация должна включать разделы: определение кибератак, методы защиты, современные технологии противодействия, важность комплексного подхода, вызовы и решения, заключение.

**Результат:**

План для презентации "Технологии и методы защиты от вредоносных программ"

1. **Введение**
   * Тема и актуальность: почему важно защищаться от кибератак.
   * Определение кибератак и примеры (фишинг, DDoS, вредоносные программы).
2. **Основные методы защиты**
   * Антивирусные программы.
   * Межсетевые экраны (файрволы).
   * Шифрование данных.
   * Обновление программного обеспечения.
3. **Технологии противодействия**
   * Системы обнаружения вторжений (IDS/IPS).
   * Искусственный интеллект и машинное обучение.
   * Блокчейн.
4. **Важность комплексного подхода**
   * Использование комбинации технологий.
   * Обучение сотрудников.
   * Регулярные аудиты и тестирование.
5. **Современные вызовы и решения**
   * Усложнение атак с использованием искусственного интеллекта.
   * Рост атак на облачные сервисы и IoT.
   * Укрепление законодательной базы и международное сотрудничество.
6. **Заключение**
   * Постоянное совершенствование технологий защиты.
   * Значимость комплексного подхода для обеспечения кибербезопасности.

Такой план позволит четко и логично изложить материалы презентации.

**Задание 9**

В введении оба плана предлагают объяснение темы и актуальности, а также определение кибератак и примеры угроз. Первый план более сжато формулирует введение, акцентируя внимание на примерах угроз, тогда как второй план делает более явный акцент на значимости защиты от кибератак, подчеркивая, почему важно защищаться.

В обоих планах перечислены антивирусные программы, межсетевые экраны, шифрование данных и обновление ПО. Разница заключается в том, что второй план уточняет термин "файрволы" для межсетевых экранов.

В современных технологиях противодействия оба плана выделяют системы обнаружения вторжений (IDS/IPS), искусственный интеллект, машинное обучение и блокчейн. В первом плане блокчейн упоминается как часть более широкого раздела "современные технологии противодействия", в то время как во втором плане он упоминается в том же контексте, но с акцентом на технологические аспекты.

В важности комплексного подхода оба плана затрагивают важность комбинирования технологий и обучения сотрудников. В первом плане также упоминается регулярный аудит безопасности, что является логичным продолжением темы, в то время как во втором плане акцент делается на регулярные аудиты и тестирование.

современных вызовах и решениях оба плана упоминают проблемы, такие как атаки с использованием искусственного интеллекта и атаки на облачные сервисы и IoT. Второй план включает несколько дополнительных фраз, например, о росте атак на IoT и акцент на укрепление законодательной базы и международного сотрудничества.

В заключении оба плана подчеркивают значимость комплексного подхода, однако в первом плане больше внимание уделяется актуальности технологий защиты, а во втором – совершенствованию технологий защиты. В общем, оба плана схожи, но второй план выглядит чуть более детализированным в некоторых аспектах (например, уточнение терминов и акцент на определенные технологии). Первый план более сжато излагает идеи и ориентирован на обзор ключевых понятий.