Инженерный вестник Дона, №3 (2026)
ivdon.ru/ru/magazine/archive/n3y2026/10840

Обеспечение конфиденциальности в генеративных мультимодальных системах: обзор современных подходов для практической реализации

Е.В Ледовская

Российский технологический университет МИРЭА

Аннотация: В статье рассмотрены основные аспекты конфиденциальности в генеративных мультимодальных системах, описаны механизмы и методы обеспечения конфиденциальности. Проведен анализ метода количественной оценки уровня конфиденциальности генеративных мультимодальных систем (ГМС). Среди наиболее продвинутых подходов к построению моделей безопасности рассмотрены STRIDE, TRIKE, OCTAVE, PASTA и VAST. Проведен анализ всех вышеупомянутых политик, моделей безопасности, моделей угроз и критериев безопасности для разработки модели для защиты конфиденциальности. В процессе моделирования угроз по методологии STRIDE для каждой из категорий угроз, было выяснено, что существующие угрозы возникают прежде всего благодаря отсутствию многофакторной аутентификации, что могло бы обеспечить от попыток получения злоумышленником информации и создание обходных аккаунтов в случае блокировки основного. Предложен общий подход к оценке конфиденциальности системы. Каждой метрике конфиденциальности отвечает набор критериев, по которым происходит оценка конфиденциальности ГМС.
Ключевые слова: конфиденциальность, информационная безопасность, оценка конфиденциальности, моделирование угроз, метрики конфиденциальности, методология моделирования угроз, система обеспечения конфиденциальности, количественная оценка, экспертный метод.

Введение

Одним из ключевых свойств, обеспечивающих гарантоспособность компьютерных систем, выступает конфиденциальность. Применительно к генеративным мультимодальным системам (ГМС) конфиденциальность трактуется как защищенность закрытой и иной конфиденциальной информации, несанкционированное раскрытие которой способно повлечь существенный материальный ущерб. Таким образом, гарантоспособная ГМС должна обеспечивать защиту как от несанкционированного использования, модификации или уничтожения информации, так и от аналогичных несанкционированных действий в отношении технических средств (компонентов системы).

Актуальность проблемы обеспечения конфиденциальности неуклонно возрастает по мере развития информационных технологий. При этом само понятие конфиденциальности и перечень сведений, относимых к конфиденциальной информации, существенно варьируются в зависимости от сферы деятельности и национальной юрисдикции.

В странах Европейского союза, например, конфиденциальность информации регулируется посредством ряда соглашений и директив, таких как директива ЕС 95/46/ЕС, 2002/58/ЕС и ETS 108, ETS 181, ETS 185, ETS 189.

Так, Конвенция о преступности в сфере компьютерной информации (ETS N 185) направлена на сдерживание, в том числе действий, направленных против конфиденциальности компьютерных данных и компьютерных сетей, систем. В соответствии с положениями настоящей Конвенции, направленными на противодействие преступлениям против конфиденциальности, доступности и целостности компьютерных данных и систем, каждая сторона принимает законодательные и иные меры, необходимые для квалификации в качестве уголовного преступления согласно ее внутреннему законодательству следующих деяний: противозаконный доступ; неправомерный перехват; воздействие на данные; воздействие на функционирование системы; противозаконное использование устройств (Конвенция о преступности в сфере компьютерной информации ETS N 185).

При анализе конфиденциальности как свойства компьютерных систем необходимо учитывать ряд ее фундаментальных особенностей:

Временная зависимость (актуальность информации). Ценность информационных активов не является константой. Существует корреляция между временем жизни информации и требуемыми усилиями по её защите: данные, обладающие высокой критичностью на момент создания системы, в процессе её эксплуатации могут девальвироваться. Данный фактор необходимо учитывать при актуализации моделей угроз и политик

безопасности, чтобы избежать нецелевого расходования ресурсов на защиту устаревших данных.

Универсальность требований к оценке ущерба. Компьютерные системы нашли применение во всех секторах, определяющих технологический суверенитет и безопасность государства. К их числу относятся теплоэнергетика, авиастроение и космическая отрасль, транспортное управление, финансовая сфера, а также органы государственной власти. Вне зависимости от отраслевой принадлежности, проектирование любой КС должно включать этап количественной и качественной оценки потенциального ущерба от утечки конфиденциальной информации. Такой подход позволяет обосновать выбор адекватных мер защиты и рассчитать экономическую эффективность системы обеспечения информационной безопасности.

Атрибутивность для современных архитектур. Обеспечение конфиденциальности является имманентно присущим (неотъемлемым) требованием для систем, построенных на основе сетевой идеологии, — открытых и распределенных систем. Высокая степень связанности и интенсивный информационный обмен в таких системах многократно увеличивают риски несанкционированного доступа. Еще более критичным это требование становится для систем критического применения (СКП), где нарушение конфиденциальности может стать триггером для каскадного развития аварий и создания чрезвычайных ситуаций.

Определение понятия конфиденциальность

В структуре информационной безопасности конфиденциальность традиционно рассматривается как один из базовых атрибутов, наряду с целостностью и доступностью (триада CIA). Её значимость многократно возрастает применительно к системам критического применения, где утрата контроля над данными может повлечь не только экономический ущерб, но и

угрозы техногенного характера, а также безопасности государства [1]. Однако, несмотря на высокую актуальность проблемы, в настоящее время наблюдается дефицит унифицированных и апробированных методик, позволяющих осуществить количественную оценку уровня конфиденциальности для гетерогенных систем, к которым относятся и генеративные мультимодальные системы (ГМС). Существующие подходы зачастую ограничиваются качественным анализом либо фрагментарной оценкой отдельных механизмов защиты, что обусловливает необходимость разработки более строгого математического и методологического аппарата.

Для анализа алгоритмов и методов обеспечения конфиденциальности необходимо привести само определение понятия конфиденциальности ГМС.

В рамках настоящего исследования под конфиденциальностью предлагается понимать имманентное свойство системы (или отдельного объекта), характеризующее её способность обеспечивать защиту от несанкционированного использования, модификации (замены) либо повреждения как информационных ресурсов, так и технических средств под воздействием внутренних и (или) внешних деструктивных факторов [2].

Исходя из приведенного определения, представляется логичным выделить два взаимосвязанных, но обладающих спецификой типа конфиденциальности:

1. **Информационная конфиденциальность** – ориентирована на защиту семантического содержания данных, циркулирующих в системе, и направлена на предотвращение их утечки, неправомерного копирования или разглашения.
2. **Техническая конфиденциальность** – касается защиты аппаратных компонентов и технических каналов передачи информации от несанкционированного доступа, перехвата или физического воздействия, которое может привести к компрометации данных.

Для перехода от качественных описаний к измеримым показателям необходимо определить метрический базис конфиденциальности. В качестве основных метрик, позволяющих комплексно охарактеризовать это свойство, предлагаются следующие:

- **Вероятность угроз ($P_{\text{у}}$)** – количественная мера, отражающая возможность реализации события, влекущего за собой нарушение конфиденциальности технических средств и (или) информации. Допустимый (приемлемый) уровень данной вероятности достигается путем внедрения комплексной системы защиты, охватывающей как информационные ресурсы, так и технические компоненты. Чем ниже значение $P_{\text{у}}$, тем выше устойчивость системы к угрозам конфиденциальности.
- **Уровень доступности ($L_{\text{Д}}$)** – метрика, характеризующая свойство технического средства или информации обеспечивать авторизованным субъектам физическую и логическую возможность своевременного изменения заданных параметров или получения доступа в строго регламентированных точках за конечный (нормативно установленный) промежуток времени. Следует подчеркнуть, что в контексте конфиденциальности доступность рассматривается не как самоцель, а как необходимое условие для легитимного управления защищаемыми ресурсами, которое реализуется, в том числе, посредством разграничения доступа на основе паролей и иных аутентификационных механизмов.
- **Уровень секретности ($L_{\text{С}}$)** – интегральная характеристика, представляющая собой совокупность взаимосвязанных организационных и технических мер, направленных на сохранение в тайне определенных сведений и параметров функционирования системы. Обеспечение секретности достигается применением средств

засекречивания (криптографического закрытия) конфиденциальных данных, а также использованием специализированных технических средств защиты информации, препятствующих её утечке по техническим каналам.

Предложенная триада метрик $(P_{\text{У}}, L_{\text{Д}}, L_{\text{С}})$ создает основу для последующего синтеза комплексного показателя конфиденциальности ГМС, учитывающего как вероятностные характеристики угроз, так и качество реализованных защитных механизмов.

Многие компании, например, такие как Hewlett Packard, Google и др., предоставляют возможность выбора настроек конфиденциальности. Для предотвращения несанкционированного доступа к личной информации или ее разглашения, обеспечения ее точности и надлежащего использования эти компании используют соответствующие физические, технические и административные процедуры.

Чтобы сформулировать некоторые более конкретные цели в вопросах конфиденциальности, необходимо определить причины ее нарушения, а именно:

- просчеты в разработке системы;
- нечеткая работа программных средств по обеспечению конфиденциальности;
- непрофессиональные действия персонала при взаимодействии с компьютерными системами (злонамеренные/случайные);
- несоблюдение административных процедур по обеспечению конфиденциальности;
- воздействие, причиненное несанкционированными пользователями или приложениями.

Реализация требования конфиденциальности в генеративных мультимодальных системах достигается путем внедрения

специализированных программно-аппаратных средств защиты информации [3]. Принципиально важным является то обстоятельство, что максимальная эффективность функционирования данных средств достигается исключительно при условии их комплексного применения, предполагающего системную интеграцию разнородных механизмов защиты в единую архитектуру безопасности. Разрозненное, фрагментарное внедрение отдельных защитных мер не позволяет сформировать устойчивый периметр безопасности и создает потенциальные бреши, которые могут быть использованы злоумышленниками для реализации атак.

Номенклатура программно-аппаратных средств, задействуемых для обеспечения конфиденциальности в ГМС, отличается значительным разнообразием и может быть классифицирована по функциональному назначению следующим образом [4]:

1. Средства криптографической защиты информации:

   – аппаратные модули и программные комплексы для шифрования речевой (голосовой) информации в каналах связи;

   – программные средства криптографического закрытия текстовых данных и иных видов информации, как при хранении, так и при передаче;

   – системы обеспечения аутентификации электронных сообщений с использованием механизмов электронной цифровой подписи, позволяющие гарантировать подлинность отправителя и целостность сообщения.

2. Средства антивирусной защиты:

   программные комплексы, обеспечивающие сигнатурный и эвристический анализ исполняемого кода и файловых объектов с целью выявления и нейтрализации вредоносного программного

обеспечения, которое может быть использовано для деструктивного воздействия на конфиденциальные данные.

3. Средства сетевой защиты:

   – системы предотвращения и обнаружения вторжений (IDS/IPS), осуществляющие мониторинг сетевого трафика и событий безопасности для своевременного выявления признаков атак;

   – средства защиты периметра сети (межсетевые экраны), реализующие фильтрацию трафика на основе заданных политик безопасности.

4. Средства защиты почтовых систем:

   специализированные программы для сокрытия, фильтрации и шифрования электронной почты, предотвращающие утечку конфиденциальной информации через каналы электронной коммуникации.

Помимо перечисленных технологических компонентов, в архитектуру корпоративных сетей, в которых функционируют ГМС, должны быть императивно включены специализированные службы, обеспечивающие поддержание режима безопасности. К их числу относятся службы информационной безопасности, службы высокой готовности (обеспечивающие отказоустойчивость), а также подсистемы централизованного мониторинга событий безопасности и администрирования средств защиты..

Подобный перечень программно-аппаратных средств, как правило, разрабатывается специалистами в области защиты информации с учетом многих факторов, например, характеристик ГМС, количества пользователей в этой системе, различия уровня доступа этих пользователей и т.д.

Ввиду того, что значительная часть современных ГМС функционирует в среде с выходом в глобальную сеть Интернет либо взаимодействует с

внешними сервисами через сетевые интерфейсы, особую актуальность приобретает проблема обеспечения безопасности компьютерных систем от внешнего сетевого воздействия [5]. Векторы сетевых атак характеризуются высокой динамикой развития: злоумышленники постоянно совершенствуют инструментарий и тактики преодоления защитных барьеров, что обусловливает необходимость непрерывной адаптации оборонительных механизмов.

Базовым элементом защиты сетевого периметра были и остаются межсетевые экраны (брандмауэры), реализующие функции фильтрации трафика на границе между доверенной внутренней сетью и внешней средой [6].

Функциональная полнота обеспечения конфиденциальности в ГМС достигается посредством реализации системы обеспечения конфиденциальности (СОК), центральное место в которой занимают механизмы идентификации, аутентификации и авторизации пользователей [7]. В СОК должны устанавливаться требования к пользователям относительно доступа к ресурсам. Данные требования включают два обязательных этапа верификации:

1. Идентификация – присвоение уникального идентификатора субъекту и сообщение его системе, что позволяет системе отличать одного пользователя от другого.
2. Аутентификация – проверка подлинности заявленного идентификатора путем сопоставления предъявленного субъектом аутентификационного фактора (знания, владения, биометрической характеристики) с эталонным значением, хранящимся в системе. Сущность данного этапа заключается в подтверждении того, что пользователь, предъявивший идентификатор, действительно является легитимным владельцем учетной записи.

СОК должны включать функции, позволяющие добавлять новых пользователей и удалять или лишать законной силы старых пользователей. Точно так же должны включаться функции для разрешения приема, изменения или проверки пользователями опознавательной информации, необходимой для проверки идентичности данного пользователя. Должны также включаться функции, которые гарантируют целостность или предотвращают неуполномоченное использование распознавательной информации, а также функции для ограничения возможности повторных попыток установить ошибочную идентичность.

Во многих СОК должны устанавливаться требования для защиты данных во время передачи по каналам связи. Такая защита обычно упоминается как защита связи в отличие от компьютерной защиты.

Конфиденциальность СОК можно оценить количеством и качеством средств, предназначенных для обеспечения конфиденциальности.

СОК ГМС могут строиться из многих компонентов. Некоторые компоненты не способствуют удовлетворению целей безопасности, другие компоненты нацелены на обеспечение безопасности. Эти компоненты считаются обеспечивающими безопасность. Наконец, могут быть некоторые компоненты, которые не обеспечивают безопасность, но все же должны работать правильно для обеспечения безопасности. Они считаются имеющими отношение к безопасности. Сочетание компонентов, обеспечивающих безопасность и имеющих отношение к безопасности, часто называют Достоверная Вычислительная База(Trusted Computing Base – TCB).

На основании определения функций СОК, которые в той или иной степени обеспечивают правильную работу системы, может быть оценена критичность этих функций. Такая классификация функций производна от анализа отказов и их последствий. Классификация функций по уровням критичности (иногда называемым уровням целостности), вместе с

максимально допустимой продолжительностью прерывания обслуживания, позволяет в процессе разработки системы выбрать соответствующие механизмы обработки ошибок и, особенно, выбрать принципы реконфигурации для обработки неисправности.

Решение задач конфиденциальности возлагается на услуги безопасности. Услуги, в зависимости от того, на решение каких задач они направлены, можно отнести к одному из трех классов.

Опорные сервисы безопасности. К данному классу относятся услуги, общие и лежащие в основе реализации большинства других услуг безопасности. Иными словами, они выступают в роли базиса для надстройки, в которую входят услуги двух других классов.

Предупреждения – это услуги безопасности, в основном ориентированные на предотвращение различного рода нарушений безопасности.

Услуги выявления нарушений и восстановления безопасности направлены прежде всего на решение задач выявления нарушений безопасности (до или после их совершения) и восстановление системы в безопасное состояние.

Опорные услуги безопасности выступают в качестве базиса для построения всех других услуг безопасности. К этому классу относятся следующие услуги безопасности.

Идентификация (присвоение имен). Однозначно идентифицируемый объект и субъекты информационных отношений являются необходимым условием для реализации большинства услуг безопасности. Идентификация обеспечивает возможность присвоения уникального идентификатора пользователям, процессам, информационным и другим ресурсам.

Управление криптографическими ключами. Данная услуга обязательна при использовании криптографических функций в любых услугах

безопасности. Под управлением ключами понимают совокупность методов и процедур, осуществляющих безопасную установку и управление ключевыми взаимоотношениями между авторизованными объектами.

Управление безопасностью и администрирование. Под управлением безопасностью понимают распространение и управление информацией, необходимой для работы услуг и механизмов безопасности. Под администрированием понимают процессы настройки параметров установки и эксплуатации программного и аппаратного обеспечения услуг безопасности, а также учет внесенных изменений в эксплуатируемое оборудование.

Защищенность системы представляет собой совокупность свойств системы, позволяющих доверять технической реализации системы [8]. Рассматривается не только качество реализуемых средств защиты, но и процедуры их разработки, способы достижения и решения технических задач.

Примерами средств защиты системы являются защита остаточной информации (или защита от повторного использования), минимизация полномочий, разделение процессов, модульность и уровни разработки, минимизация круга знающих лиц и т.д.

Остаточная информация – информация на устройстве памяти, оставшаяся от формально удаленных операционной системой данных. Информация может остаться из-за формального удаления файла или из-за физических свойств запоминающих устройств. Остаточная информация может привести к случайному распространению конфиденциальной информации, если хранилище данных окажется вне зоны контроля (например, будет удалено или передано третьей стороне). В настоящее время, чтобы избежать появления остаточной информации, применяется множество методов. В зависимости от эффективности и назначения они подразделяются на «очистку» и «уничтожение» такой информации. Конкретные методики

используют перезаписывание, размагничивание, шифрование и физическое уничтожение.

Обеспечение конфиденциальности на качественном уровне предполагает неукоснительное следование политике конфиденциальности, которая представляет собой формализованную совокупность условий и правил, регламентирующих доступ авторизованных пользователей к информации и ресурсам ГМС. Указанные условия конкретизируются в виде требований безопасности, подлежащих обязательной имплементации в рамках системы обеспечения конфиденциальности (СОК) ГМС.

Реализация политики конфиденциальности осуществляется посредством задействования соответствующих механизмов защиты, к числу которых относятся процедуры идентификации и аутентификации субъектов доступа, механизмы распределения ресурсов, а также средства обеспечения отказоустойчивости и непрерывности функционирования. В структуре механизмов конфиденциальности традиционно выделяются две основные категории компонентов: автоматизированные (программно-аппаратные) и организационные (административные) [9].

Автоматизированные компоненты, как правило, интегрированы непосредственно в вычислительную среду ГМС и включают реализацию соответствующих процедур как на стороне пользователя, так и на стороне администратора безопасности, обеспечивая тем самым непрерывность и непротиворечивость применения установленных политик.

Общим для моделей обеспечения конфиденциальности является то, что все они направлены на введение определенных обязательных процедур анализа конфиденциальности, программ, средств, ресурсов и пользователей, взаимодействующих с ГМС.

Критерии конфиденциальности рассматривают угрозы, связанные с несанкционированным ознакомлением с информацией в которой

предусмотрены следующие услуги: доверительная конфиденциальность, административная конфиденциальность, повторное использование объектов, анализ скрытых каналов и конфиденциальность при обмене.

Краткое изложение каждой из услуг критериев конфиденциальности:

а) доверительная конфиденциальность дает возможность пользователю управлять информационными потоками, что идут от защищенных объектов, что принадлежат его домена, других пользователей. Уровни данной услуги варьируются из полноты защиты и избирательности управления;

б) административная конфиденциальность позволяет администраторам или уполномоченным пользователям управлять потоками информации от объектов к пользователям. Аналогично доверительнойя конфиденциальности уровни данной услуги варьируются на основании полноты защиты и избирательности управления;

в) повторное использование объектов предполагает обеспечение правильного повторного использования разделяемых объектов с гарантиями отсутствия информации, остающейся после пользователя или процесса, если один из них (объект) предоставляется следующему конкретному пользователю или процессу;

г) анализ скрытых каналов выполняется с целью выявления и устранения существующих, но не контролируемых другими услугами потоков информации. Уровни данной услуги формируются на основе того, выполняются только обнаружение, контроль и перекрытие скрытых каналов;

д) конфиденциальность при обмене заключается в обеспечении защиты объектов от несанкционированного доступа к информации, что содержится в этих объектах, в процессе импорта через незащищенные каналы.

Модели угроз и подходы по формированию модели безопасности

Среди более распространенных методологий построения модели угроз различают следующие: STRIDE (Spoofing, Tampering, Repudiation, Information

Disclosure, Denial of Service, Elevation of Privilege — подмена, изменение данных, отказ от авторства, раскрытие информации, отказ в обслуживании, повышение привилегий), TRIKE (Trike Risk Methodology — методология управления рисками «Трайк»), OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation — оперативно-критическая оценка угроз, активов и уязвимостей), PASTA (Process for Attack Simulation and Threat Analysis — процесс симуляции атак и анализа угроз) и VAST (Visual, Agile, and Simple Threat modeling — визуальное, гибкое и простое моделирование угроз). Рассмотрим особенности каждой из методик.

Метод STRIDE

STRIDE была разработана Лореном Конфельдером и Праэритом Гаргом в 1999 году с целью определения потенциальных уязвимостей и угроз для продуктов компаний. Методология направлена на обеспечение соответствия приложений требованиям безопасности по конфиденциальности, целостности и доступности, кроме авторизации, аутентификации и безотказности.

Методология STRIDE, получившая широкое распространение в практике моделирования угроз, позволяет не только идентифицировать потенциальные уязвимости, но и определить соответствующие методы их нейтрализации. Относительная простота применения данной методологии сочетается с существенными временными затратами, что необходимо учитывать при планировании соответствующих работ [10, 11].

Методология TRIKE

TRIKE – это открытая методология анализа угроз, которая сосредотачивается на аудиторском процессе с точки зрения управления рисками и защиты. Этот Подход учитывает реализацию, угрозы и модели рисков, обеспечивая приемлемый уровень риска для каждого актива для заинтересованных сторон.

Основная цель методологии TRIKE заключается в обеспечении приемлемого уровня риска для всех заинтересованных сторон (стейкхолдеров). В рамках данного подхода решаются задачи информирования участников о характере и влиянии выявленных рисков, а также содействия в осмыслении и минимизации этих рисков для организации. Архитектура методологии предусматривает возможность координации и совместной работы пользователей за счет встроенных механизмов приоритизации мер по нейтрализации угроз и наличия автоматизированных компонентов.

В основе TRIKE лежит анализ диаграмм потоков данных, которые наглядно отражают информационные взаимодействия в системе и позволяют пользователям моделировать различные сценарии функционирования. Методология предоставляет инструментарий для идентификации рисков, присвоения им количественных или качественных значений, а также для разработки комплекса защитных мер, направленных на предотвращение потенциальных угроз.

Вместе с тем следует отметить, что применение TRIKE в крупных системах может быть сопряжено с определенными трудностями, обусловленными необходимостью глубокого понимания архитектуры и всех взаимосвязей анализируемой системы в целом.

Метод OCTAVE

OCTAVE — методология оценки организационных рисков, таких как влияние утечки данных на операционную деятельность компании. Разработанная Университетом Карнеги-Меллона (США) и CERT Института программной инженерии (SEI) в 2003 году, она ориентирована на малые и средние предприятия до 100 человек.

Методология OCTAVE базируется на принципе самостоятельного управления (self-directed approach), в рамках которого сотрудники

организации — преимущественно представители руководящего звена и операционных команд — самостоятельно определяют стратегию обеспечения безопасности. Такой подход, будучи эффективным для вовлечения персонала в процессы управления рисками, объективно усложняет масштабирование методологии, что обусловливает её ориентацию преимущественно на малые и средние предприятия.

К числу основных преимуществ OCTAVE относится её способность способствовать выявлению методов снижения рисков, повышению уровня осведомленности сотрудников в области риск-менеджмента, а также укреплению механизмов командного взаимодействия. Методология характеризуется сниженной потребностью в объемной документации, высокой степенью конфигурируемости под специфику организации и обеспечивает формирование репрезентативного обзора деятельности с получением воспроизводимых (последовательных) результатов.

Метод PASTA

Процесс симуляции атак и анализа угроз (PASTA) – это ориентированная на риски методология моделирования угроз, разработанная генеральным директором VerSprite Тони Уседа-Велезом и лидером по безопасности Марко М. Мораном. PASTA имеет предпочтение масштабируемости, что делает ее идеальной для растущих бизнесов и может привлекать технические команды и ключевые лица, принимающие решения, обеспечивая соблюдение требований соответствия и регуляторных потребностей, а также учет технического объема и потенциальных уязвимостей.

PASTA позволяет контекстуальный подход, при котором технические действия всегда связаны с бизнес-целями и обеспечивает моделирование угроз на основе доказательств, поддерживая мотивы угроз и используя данные [11].

Согласно методологии разработки модели угроз PASTA предлагается 7-шаговый процесс анализа рисков, что складывается с таких действий:

- определение целей;
- определение технического объема;
- декомпозиция приложению;
- анализ угроз;
- анализ уязвимостей и слабых мест;
- моделирование атак;
- анализ рисков и влияния.

Метод VAST

Методология VAST представляет собой подход к моделированию угроз, разработанный авторами программного продукта ThreatModeler. Её целевая направленность заключается в решении проблем масштабирования корпоративных систем с помощью организации моделирования угроз в полный жизненный цикл разработки программного обеспечения. В основе VAST лежат три ключевых компонента, обеспечивающих реализацию масштабируемого решения для анализа угроз.

Автоматизация призвана минимизировать дублирование задач в процессах моделирования угроз и обеспечить непрерывность соответствующих процедур.

Интеграция предусматривает согласованное взаимодействие инструментальных средств на всех этапах жизненного цикла порграммного обеспечения, а также поддержку гибких методологий разработки и эксплуатации (DevOps).

Сотрудничество (коллаборация) предполагает вовлечение в процесс ключевых стейкхолдеров — разработчиков приложений, системных архитекторов, специалистов по безопасности и высшего руководства, что обеспечивает учет разнородных требований и перспектив.

Разработка модели обеспечения конфиденциальности

Для разработки модели угроз была выбрана методология STRIDE, ведь она характеризуется гибкостью и сосредотачивается на анализе дизайна да архитектуры, что имеет смысл в случае продуманного дизайна сайта, а также обязательностью проверок кода и дизайна.

Для каждой из 6 компонент методологии STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial Of Service, Elevation Of Privileges) будет разработана таблица угроз с учетом происхождения нарушителей (внешние или внутренние), свойства, на которую направлена угроза, характер угрозы (преднамеренные и непреднамеренные). идентификационный номер угрозы, подробное описание сущности угрозы, активы, находящиеся под влиянием этой угрозы.

1. Подмена личности (Spoofing)

Моделирование угроз категории «Подмена личности» направлено на выявление и анализ сценариев, связанных с незаконной аутентификацией злоумышленника в системе под видом легитимного пользователя или доверенного субъекта. Угрозы данного типа реализуются посредством различных технологий и методов обхода механизмов идентификации, включая кражу учетных данных, использование украденных сертификатов, подделку идентификаторов сессий, а также применение методов социальной инженерии для получения конфиденциальной аутентификационной информации.

Применительно к архитектуре ГМС угрозы подмены личности могут проявляться как:

– несанкционированный доступ к учетным записям пользователей с последующим совершением действий от их имени (публикация контента, изменение настроек, инициирование транзакций);

– использование поддельных токенов доступа для обхода механизмов аутентификации в распределенной среде.

Основной целью реализации угроз данной категории является не только получение несанкционированного доступа к ресурсам, но и последующая компрометация репутации легитимных пользователей путем совершения противоправных или деструктивных действий от их имени. Особую опасность представляет возможность использования скомпрометированной учетной записи для развития дальнейших атак на другие компоненты ГМС.

2. Смена данных (Tampering)

Моделирование угроз категории «Модификация данных» ориентировано на выявление сценариев несанкционированного изменения информации или исполняемого кода в процессе их хранения, передачи или обработки. Угрозы данного типа реализуются путем внедрения в информационные потоки, перехвата и модификации транзакций, изменения содержимого баз данных, а также подмены программного кода в репозиториях или в оперативной памяти исполняемых сред.

Специфика функционирования ГМС предполагает проявления угроз модификации данных следующим образом:

– несанкционированное изменение параметров учетных записей пользователей (прав доступа, персональных данных, аутентификационных атрибутов);

– подмена программного кода компонентов системы для внедрения вредоносной логики.

Последствиями реализации угроз данной категории могут выступать нарушение целостности обрабатываемых данных, искажение результатов функционирования ГМС, а также инициирование каскадных сбоев в работе зависимых компонентов. В ряде сценариев модификация данных может использоваться как подготовительный этап для реализации атак других

категорий, например, для последующего отказа в обслуживании или повышения привилегий.

3. Отказ от авторства (Repudiation)

Моделирование угроз категории «Отказ от авторства» направлено на выявление сценариев, в которых субъект (пользователь, процесс или система) имеет возможность отрицать факт совершения определенных действий в информационной системе. Угрозы данного типа связаны с недостаточностью или отсутствием механизмов неоспоримости, обеспечивающих доказательственную базу для идентификации источника действий и их временной привязки.

В рамках ГМС угрозы отказа от авторства могут реализовываться следующими способами:

– использование средств шифрования каналов связи, затрудняющих идентификацию источника передаваемых данных;

– маскировка сетевых атрибутов посредством подмены IP-адресов, применения анонимизирующих прокси-серверов или технологий луковой маршрутизации;

– преднамеренное удаление или модификация записей в системных журналах после совершения противоправных действий.

Особенностью угроз данной категории является их вторичный характер: отказ от авторства, как правило, сопутствует реализации других типов атак (несанкционированный доступ, модификация данных), затрудняя их расследование и привлечение виновных к ответственности. Обеспечение неоспоримости действий в ГМС требует внедрения механизмов электронной цифровой подписи, надежного протоколирования с защитой от модификации логов, а также применения методов криптографической привязки действий к уникальным идентификаторам субъектов.

4. Раскрытие информации (Information Disclosure)

Моделирование угроз категории «Раскрытие информации» ориентировано на выявление сценариев несанкционированного ознакомления с конфиденциальными данными, подлежащими защите. Угрозы данного типа предполагают нарушение конфиденциальности как целенаправленными действиями злоумышленников, так и вследствие непреднамеренных ошибок пользователей или администраторов, а также технических уязвимостей программно-аппаратного обеспечения.

Анализ угроз раскрытия информации в ГМС позволяет выделить следующие характерные сценарии их возникновения и развития:

Преднамеренное раскрытие:

– несанкционированный доступ к базам данных, содержащим конфиденциальную информацию пользователей (персональные данные, история взаимодействий, биометрические образцы);

– эксплуатация уязвимостей программного кода, позволяющих обойти механизмы контроля доступа;

– раскрытие служебной информации о внутренней архитектуре ГМС (исходный код, конфигурационные параметры, сведения об известных уязвимостях), что создает предпосылки для реализации атак других категорий.

Непреднамеренное раскрытие:

– ошибочные действия пользователей, приводящие к публикации конфиденциальных данных в открытых источниках или их передаче неуполномоченным лицам;

– остаточная информация на высвобождаемых носителях или в повторно используемых областях памяти при отсутствии механизмов гарантированного удаления.

Особую значимость угрозы раскрытия информации приобретают в контексте мультимодальных систем, обрабатывающих чувствительные данные различных типов (биометрические образцы, голосовые слепки,

персональные изображения), компрометация которых может привести к необратимым последствиям для субъектов данных.

5. Отказ в обслуживании (Denial Of Service)

Моделирование угроз категории «Отказ в обслуживании» ориентировано на выявление сценариев, приводящих к временной или постоянной утрате способности системы предоставлять сервис легитимным пользователям. Угрозы данного типа реализуются путем исчерпания вычислительных ресурсов, эксплуатации уязвимостей, приводящих к аварийному завершению процессов, либо целенаправленного нарушения функционирования критических компонентов инфраструктуры.

В контексте ГМС угрозы отказа в обслуживании может проявиться в компрометации учетной записи пользователя с последующими действиями, провоцирующими блокировку (например, массовое изменение настроек профиля или публикация запрещенного контента, что система распознает как нарушение политик использования). В таком сценарии атака, начавшаяся как подмена личности или модификация данных, перерастает в отказ в обслуживании для законного владельца учетной записи вследствие автоматической или административной блокировки.

6. Незаконное повышение привилегий (Elevation of Privileges)

Моделирование угроз категории «Повышение привилегий» направлено на выявление сценариев, в которых субъект (пользователь или процесс) получает несанкционированный доступ к функциональным возможностям и ресурсам, превышающим его установленные полномочия. Угрозы данного типа реализуются путем эксплуатации уязвимостей в механизмах разграничения доступа, некорректной конфигурации политик безопасности либо использования скомпрометированных учетных записей с высокими привилегиями.

Рассматривая ГМС как объект угроз, можно идентифицировать следующие ключевые формы повышения привилегий:

Вертикальное повышение привилегий: получение доступа к функциям, предназначенным для пользователей с более высоким уровнем полномочий (например, рядовой пользователь получает права администратора, модератора или редактора контента). Это достигается путем:

– эксплуатации уязвимостей в механизмах авторизации;

– перехвата и модификации токенов доступа;

– компрометации учетной записи пользователя, обладающего расширенными правами.

Горизонтальное повышение привилегий: получение доступа к ресурсам и функциям другого пользователя с аналогичным уровнем полномочий (например, доступ к личным данным или сессиям других пользователей). Реализуется через:

– подмену идентификаторов сессий;

– эксплуатацию уязвимостей в механизмах изоляции данных между пользователями;

– использование недостатков в реализации многопользовательского доступа.

Особую опасность угрозы повышения привилегий представляют в ГМС, где различные категории пользователей обладают дифференцированными правами на генерацию, модификацию и публикацию контента. Получение злоумышленником административных привилегий может привести к полной компрометации системы, включая возможность предоставления высоких полномочий другим субъектам, что создает эффект "снежного кома" и многократно увеличивает масштаб потенциального ущерба. Представим эти данные в виде таблицы (таблица №1) [11].

Таблица № 1

Угрозы и уязвимости ГМС в соответствии с моделью STRIDE

Угроза ГМС	Уязвимость	Возможное решение
Подмена	Возможность входить в качестве контроллера, коммутатора или приложения ввиду отсутствия средств защиты или ошибок в ПО.	Внедрение обязательных процедур аутентификации в рабочих операциях.
Модификация	Злоумышленник может перезаписать политики контроллера. Перехват и модификация управляющих сообщений Open Flow может иметь негативные последствия для конфигурации сети.	Внедрение механизмов контроля и проверки на северном и южном интерфейсах ГМС. Важные действия выполняются после верификации независимыми элементами управления.
Отказ от авторства	Отсутствие мониторинга состояния коммутаторов и управляющего программного обеспечения может открыть возможности для выполнения скрытых операций.	Уникальная идентификация элементов ГМС. Механизмы журналирования и отслеживания должны выполняться автоматически и должны быть защищены.
Раскрытие информации	Централизованное хранение информации упрощает сбор данных о структуре сети. Компрометация серверного программного обеспечения может привести к раскрытию учетных данных и сетевой базы.	Перемещение коммуникаций ГМС на отдельные защищенные каналы. Контроллер и хранилище данных должны быть удалены из сети передачи данных.
Отказ в обслуживании	Функциональность коммутаторов зависит от единого контроллера и канала управления, который подвержен множеству атак, а также ошибки в ПО. Таблицы коммутации при этом ограничены и быстро переполняются.	Развертывание контроллера в сочетании с механизмами обнаружения вторжений; использование механизмов восстановления и избыточности сетевых узлов.

Оценка конфиденциальности системы

Предлагается наиболее общий подход к оценке конфиденциальности системы. Каждой метрике конфиденциальности отвечает набор критериев, по которым происходит оценка конфиденциальности ГМС (таблица №2). Набор критериев может быть изменен в зависимости от назначения и специфики функционирования конкретной ГМС.

Таблица № 2

Основные метрики и критерии оценки конфиденциальности ГМС

Метрики конфиденциальности	Наименование критерия
Вероятность угроз $Р$у – вероятность нарушений конфиденциальности технических средств и (или) информации	Наличие функций идентификации и аутентификации
	Наличие функций проверки сохранения конфиденциальных данных
	Наличие функций контроля соблюдение конфиденциальности
	Наличие функций восстановление конфиденциальности
	Наличие функций мониторинга и оповещение нарушений конфиденциальности
Уровень доступности $L_Д$ – способность системы обеспечивать физический защита от возможности изменения заданных параметров технических и (или) информационных ресурсов в заданных точках за конечное время	Наличие паролей доступа к информационным ресурсам
	Наличие распределения зон (уровней) доступа между пользователями
	Наличие стойкости функционирование при ошибках пользователя, связанных с конфиденциальностью
Уровень секретности $L_С$ – характеристика способности системы сохранять секретность технических и (или) информационных ресурсов	Наличие технических средств защиты информации
	Наличие защиты от несанкционированного доступа
	Наличие криптографических средств защиты информации

Для определения комплексной количественной оценки уровня гарантоспособности системы в целом определяются комплексные оценки ее

основных атрибутов. Комплексную оценку конфиденциальности определим с помощью среднего арифметического, которое определяется по формуле [12]:

$$A_{\text{конф}} = \sum_{j=1}^{m} \mathrm{g}_j L_j \qquad (1)$$

L_j – многочисленное значение j-той метрики конфиденциальности;

g_j – весовой коэффициент j-той метрики конфиденциальности;

m – количество показателей конфиденциальности.

Весовые коэффициенты g_j учитывают важность каждой метрики среди других и определяются экспертным методом:

$$(\sum_{j=1}^{m} \mathrm{g}_j = 1)$$

Метрики конфиденциальности имеют качественный вид представления, поэтому для определения их комплексной оценки используется экспертный метод с ранжированием по трехуровневой шкале.

Конфиденциальность характеризуется тремя метриками: вероятность угроз $P_У$, уровень доступности $L_Д$, уровень секретности $L_С$.

В качестве примера определим комплексную оценку вероятности угроз $P_У$.

Экспертным методом определяем уровень критериев оценки вероятности угроз. При этом обозначим: B – высокий уровень; C – средний уровень; H – низкий уровень. Комплексная оценка вероятности угроз определяется формулой (2) [6]:

$$P_{\text{у}} = 1 - \sum_{j=1}^{\mathrm{m}_H} \mathrm{g}_{Hj} - 0{,}5 \sum_{j=1}^{\mathrm{m}_C} \mathrm{g}_{\mathrm{C}j} \qquad (2)$$

m_H – число показателей низкого уровня;

m_C – число показателей среднего уровня;

g_{Hj} – нормированный критерий низкого уровня;

g_{Cj} – нормированный критерий среднего уровня.

Требования нормирования сводятся к тому, чтобы сумма весов всех критериев равнялась единице. Критерии оценки вероятности угроз обозначим следующим образом:

K_1 – наличие функций идентификации и аутентификации;

K_2 – наличие функций проверки сохранности конфиденциальных данных;

K_3 – наличие функций контроля соблюдения конфиденциальности;

K_4 – наличие функций восстановления конфиденциальности;

K_5 – наличие функций мониторинга и оповещения нарушений конфиденциальности.

В таблице №3 в качестве примера приведены уровни критериев вероятности угроз, проставленных всеми экспертами. Определим комплексную оценку вероятности угроз $P_У$ при значениях весовых коэффициентов, которые также определяются экспертами, для вышеозначенных критериев:

$$g_1 = 0{,}25; g_2 = 0{,}12;\ g_3 = 0{,}13;\ g_4 = 0{,}25; g_5 = 0{,}25.$$

Таблица № 3

Экспертная таблица ранжирования критериев оценки вероятности угроз

Эксперты	K_1	K_2	K_3	K_4	K_5
1	В	Н	С	В	В
2	С	Н	Н	В	С
3	В	С	Н	С	В
4	С	С	С	В	С
5	В	С	Н	С	В
6	В	Н	С	С	В
7	В	С	Н	В	В

Количество критериев низкого уровня равно $n_н = 7$. Пронумеруем вес критериев низкого уровня:

$$g_{2,c} = \frac{0,12 * 3}{7} = 0,051;\ g_{3,c} = \frac{0,13 * 4}{7} = 0,074$$

Количество критериев среднего уровня равно n_c =14. Прономеруем значимость критериев среднего уровня:

$$g_{1,c} = \frac{0,25 * 2}{7} = 0,071;\ g_{2,c} = \frac{0,12 * 4}{7} = 0,069;\ g_{3,c} = \frac{0,13 * 3}{7} = 0,056;$$

$$g_{4,c} = \frac{0,25 * 3}{7} = 0,11;\ g_{5,c} = \frac{0,25 * 2}{7} = 0,071;$$

Подставив прономерованные значимости критериев в формулу (2), получим комплексную оценку вероятности угроз $P_у$.

$$P_у = 1 - (0,051 + 0,074) - 0,5(0,071 + 0,069 + 0,56 + 0,11 + 0,07 = 0,6865$$

Аналогично определяются комплексные оценки уровня доступности $L_д$ и уровня секретности $L_с$. Комплексная оценка уровня конфиденциальности определяется по формуле (1).

Результаты

Для достижения поставленных целей и решения задач исследования был применен комплекс взаимодополняющих методов.

1. Теоретический анализ: проведено изучение и синтез существующих определений конфиденциальности, её метрик, причин нарушений и классификации услуг безопасности (опорные, предупреждения, выявления и восстановления).

2. Моделирование угроз: применена методология STRIDE для систематического выявления и классификации угроз конфиденциальности в ГМС. Методология включает анализ угроз по шести компонентам: подмена, модификация, отказ от авторства, раскрытие информации, отказ в обслуживании, повышение привилегий.

3. Экспертные оценки: использован экспертный метод для:

- ранжирования критериев оценки метрик конфиденциальности по трехуровневой шкале (высокий, средний, низкий уровень);
- определения весовых коэффициентов (g_j) для каждой метрики в комплексной оценке.

4. Количественная оценка: разработан математический аппарат для расчета комплексной оценки конфиденциальности на основе средневзвешенного значения её метрик (вероятность угроз, уровень доступности, уровень секретности), которые, в свою очередь, рассчитываются на основе экспертных оценок критериев.

На основе применения указанных методов были получены следующие результаты.

Сформировано определение конфиденциальности для ГМС как свойства системы обеспечивать защиту информации и технических средств от несанкционированных действий.

Выделены и описаны метрики конфиденциальности ($P_{\text{У}}, L_{\text{Д}}, L_{\text{С}}$) и соответствующие им критерии оценки (например, для $P_{\text{У}}$: наличие функций идентификации, контроля, восстановления и т.д.).

Обоснован выбор методологии STRIDE для моделирования угроз в ГМС в силу её гибкости и ориентации на анализ архитектуры.

Разработана модель угроз для ГМС по методологии STRIDE, представленная в виде структурированного перечня угроз, уязвимостей и возможных решений (Таблица 1).

Предложена методика количественной оценки конфиденциальности, включающая:

- экспертное ранжирование критериев по каждой метрике;
- формулы для расчета комплексных оценок по каждой метрике (например, $P_{\text{У}}$ по формуле (2));

- формулу (1) для вычисления итоговой комплексной оценки конфиденциальности системы ($А_{конф}$);
- на практическом примере продемонстрирован расчет вероятности угроз ($P_у = 0.6865$) на основе смоделированных экспертных данных (таблицы № 2 и 3).

Заключение

Конфиденциальность ГМС сводится к разработке мероприятий, направленных на обеспечение сохранности и строго регламентированной доступности технических и информационных ресурсов. Все условия и параметры конфиденциальности устанавливаются на этапах разработки и проектирования ГМС и, в основном, сводятся к установлению разного уровня доступа персонала к информации с разной степенью секретности и использованию программно-аппаратных средств защиты информации. Для каждой ГМС разрабатывается политика конфиденциальности, которая базируется на определенных методах и механизмах обеспечения конфиденциальности. В работе впервые предложен подход к количественной оценке уровня конфиденциальности ГМС, который может применяться для систем самого разнообразного назначения, включая системы критического использования. Полученная таким образом количественная оценка конфиденциальности позволит в дальнейшем осуществить количественную оценку уровня гарантоспособности генеративных мультимодальных систем в целом.

Проведенное исследование подтверждает актуальность задачи разработки методик количественной оценки конфиденциальности для сложных систем, таких как ГМС. В работе предложен структурированный подход, сочетающий:

- качественный анализ на основе моделирования угроз (методология STRIDE), что позволяет системно выявить и классифицировать потенциальные уязвимости.
- количественную оценку на основе экспертных методов, что дает возможность получить измеримый показатель уровня конфиденциальности системы.

Предложенная модель и методика оценки носят адаптивный характер: набор критериев и весовые коэффициенты могут быть скорректированы в зависимости от специфики и назначения конкретной системы. Это позволяет использовать разработанный подход для сравнительного анализа различных систем или для мониторинга изменения уровня конфиденциальности одной системы во времени. Результаты работы могут служить основой для формирования требований к системе обеспечения конфиденциальности и выбора адекватных программно-аппаратных средств защиты информации.

Литература

1. Багаутдинов Т.И. Анонимизация данных как средство обеспечения конфиденциальности в системах искусственного интеллекта // Новые информационные технологии в нефтегазовой отрасли и образовании. Материалы XII Международной научно-практической конференции-конкурса. В 2-х томах. . - Тюмень: 2025. - С. 207-211.

2. Ананьев А.А. Конфиденциальность персональных данных в информационном обществе и их использование третьими лицами // Устойчивое развитие и кооперация: содействие внедрению инноваций. сборник трудов II всероссийской научно-практической конференции студентов, аспирантов и молодых ученых. - Москва: 2022. - С. 593-598.

3. Смирнов В.М., Филиппова П.И. Обеспечение информационной безопасности для защиты компьютерных и сетевых данных // STUDNET, -

2021. - Т. 4. № 5. URL: cyberleninka.ru/article/n/obespechenie-informatsionnoy-bezopasnosti-dlya-zaschity-kompyuternyh-i-setevyh-dannyh?ysclid=mm6gm3kuxi668667685

4. Рыбаков С.Ю., Ташлыков Ф.А. Анализ подходов к обнаружению атак нулевого дня в сетях интернета вещей // Инженерный вестник Дона, 2025, № 7. URL: ivdon.ru/ru/magazine/archive/n7y2025/10202

5. Плешакова Е.С., Карпенко Н.Э., Гомбоев С.М. Анализ и оценка угроз безопасности и конфиденциальности в сетях 5G с использованием машинного обучения // Вопросы обеспечения безопасности в киберпространстве. материалы Всероссийской научно-технической конференции. - Махачкала: 2022. - С. 310-315.

6. Кулакова Е.С., Труханов Д.А. Современные средства защиты информации в беспроводных сетях // Достижения и перспективы научных исследований молодежи. Материалы XXII научно-практической конференции с международным участием. - Уфа: 2024. - С. 278-283.

7. Кунин Н.Т. Моделирование взаимодействия элементов корпоративной сети с мобильными устройствами пользователей // Кибербезопасность: технические и правовые аспекты защиты информации. Сборник научных трудов по итогам III ежегодной национальной научно-практической конференции. - Москва: 2024. - С. 292-299.

8. Чибинев Н.Н., Ляшенко Н.В. Кибератака как новый вид чрезвычайных ситуаций // Инженерный вестник Дона, 2024, № 7. URL: ivdon.ru/ru/magazine/archive/n7y2024/9323

9. Горин Д.С., Шатовкин Р.Р. Исследование принципов построения и основных элементов экосистем информационной безопасности // Инженерный вестник Дона, 2026, № 1. URL: ivdon.ru/ru/magazine/archive/n1y2026/10648

10. Allen-Addy C. Threat Modeling Methodology: STRIDE. IriusRisk. // URL: iriusrisk.com/resources-blog/threat-modeling-methodology-stride

11. Software Engineering Institute, Threat Modeling: 12 Available Methods // URL: insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/.

12. Ghalebikesabi S., Berrada L., Gowal S., Ktena I., Stanforth R., Hayes J., De S., Smith S. L., Wiles O., Balle B. Differentially Private Diffusion Models Generate Useful Synthetic Images // URL: arxiv.org/pdf/2302.13861.

References

1. Bagautdinov T.I. Materialy XII Mezhdunarodnoj nauchno-prakticheskoj konferencii-konkursa. V 2-h tomah. Tyumen, 2025, pp. 207-211.

2. Anan'ev A.A. Sbornik trudov II vserossijskoj nauchno-prakticheskoj konferencii studentov, aspirantov i molodyh uchenyh. Moskva, 2022, pp. 593-598.

3. Smirnov V.M., Filippova P.I. StudNET, 2021. Vol. 4. No. 5. URL: cyberleninka.ru/article/n/obespechenie-informatsionnoy-bezopasnosti-dlya-zaschity-kompyuternyh-i-setevyh-dannyh?ysclid=mm6gm3kuxi668667685

4. Rybakov S.Yu., Tashlykov F.A. Inzhenernyj vestnik Dona, 2025, №. 7. URL: ivdon.ru/ru/magazine/archive/n7y2025/10202.

5. Pleshakova E.S., Karpenko N.E., Gomboev S.M. Voprosy obespecheniya bezopasnosti v kiberprostranstve. materialy Vserossijskoj nauchno-tekhnicheskoj konferencii. Makhachkala, 2022, pp. 310-315.

6. Kulakova E.S., Trukhanov D.A. Dostizheniya i perspektivy nauchnyh issledovanij molodezhi. Materialy XXII nauchno-prakticheskoj konferencii s mezhdunarodnym uchastiem. Ufa, 2024, pp. 278-283.

7. Kunin N.T. Kiberbezopasnost': tekhnicheskie i pravovye aspekty zashchity informacii. Sbornik nauchnyh trudov po itogam III ezhegodnoj nacional'noj nauchno-prakticheskoj konferencii. Moskva, 2024, pp. 292-299.

8. Chibinev N.N., Lyashenko N.V. Inzhenernyj vestnik Dona, 2024, № 7. URL: ivdon.ru/ru/magazine/archive/n7y2024/9323.

9. Gorin D.S., Shatovkin R.R. Inzhenernyj vestnik Dona, 2026, № 1. URL: ivdon.ru/ru/magazine/archive/n1y2026/10648.

10. Allen-Addy C. Threat Modeling Methodology: STRIDE. IriusRisk. Available at: iriusrisk.com/resources-blog/threat-modeling-methodology-stride.

11. Software Engineering Institute. Threat Modeling: 12 Available Methods. December 03, 2018. URL: insights.sei.cmu.edu/blog/threat-modeling-12-available-methods.

12. Ghalebikesabi S., Berrada L., Gowal S., Ktena I., Stanforth R., Hayes J., De S., Smith S.L., Wiles O., Balle B. Differentially Private Diffusion Models Generate Useful Synthetic Images. URL: arxiv.org/pdf/2302.13861.

Авторы согласны на обработку и хранение персональных данных.

Дата поступления: 10.01.2026

Дата публикации: 3.03.2026