DOI: 10.58168/PPSPM2025_332-337
УДК 004.056

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ САПР

О.А. Рожкова, Д.Е. Орлова

ФКОУ ВО Воронежский институт ФСИН России

В работе приводятся рассуждения на тему роли информационной безопасности при использовании САПР. Приводится классификация известных уязвимостей и проводится их анализ: выявляются причины возникновения указанных уязвимостей, потенциальные риски последствия. На основе проведенного анализа делается вывод о мерах, которые необходимо использовать при работе с САПР, касаемо безопасности информации.

Ключевые слова: система автоматизированного проектирования, информационная безопасности, уязвимость, угроза данных, защита данных.

ENSURING INFORMATION SECURITY WHEN USING CAD

O.A. Rozhkova, D.E. Orlova

Voronezh Institute of the Federal Penitentiary Service of Russia

The paper discusses the role of information security when using CAD. It provides a classification of known vulnerabilities and analyzes them, identifying the causes of these vulnerabilities and potential risks. Based on this analysis, the paper concludes on the measures that should be taken when working with CAD in terms of information security.

Keywords: computer-aided design system, information security, vulnerability, data threat, data protection.

Обеспечение информационной безопасности (ИБ) становиться критически важным аспектом в условиях современной геополитической ситуации. Особенно это относится к тем отраслям промышленности, где используют системы автоматизированного проектирования (САПР). САПР, как отмечает CNews, "больше всего востребован в строительстве и смежных отраслях… компьютер заменил кульман, поэтому везде, где раньше чертили на бумаге, теперь рисуют при помощи клавиатуры и мыши"[1].

Современные САПР – критические информационные активы. В них заключается интеллектуальная собственность, модели изделий, конструкторская документация, спецификация, а также лицензии. Все это формирует задачу эффективной системы защиты информации.

В настоящий момент доступ россиян к иностранным САПР затруднен. Ключевые зарубежные разработчики САПР, такие как Autodesk, Siemens DIS, Dassault Systemes Solidworks, покинули российский рынок, прекратив продажу новых лицензий и поддержку существующих пользователей. Данный факт открывает возможности для развития отечественных решений, однако влечет за собой риски. Они возникают в результате того, что любая утечка или компрометация конфиденциальной информации (конструкторская документация, технологические процессы, результаты моделирования и анализа), обрабатываемой в САПР, может привести к серьезным экономическим потерям, нарушению конкурентоспособности, а в некоторых случаях – и к угрозе национальной безопасности.

Целью нашего исследования является выявление и анализ угроз информационной безопасности, связанных с использованием САПР, и разработка рекомендаций по мерам защиты для минимизации рисков.

Для достижения поставленной цели необходимо решить следующие задачи:

1) классифицировать угрозы ИБ, возникающие при использовании САПР;
2) проанализировать возникающие последствия указанных угроз и оценить наносимый ущерб для предприятия;
3) разработать рекомендаций по организации системы защиты информации в САПР.

Нам удалось классифицировать угрозы безопасности информации при использовании САПР следующим образом:

1) угрозы, связанные с уязвимостями САПР;

2) угрозы, связанные с вредоносным программным обеспечением (ВПО);

3) угрозы, связанные с хранением и передачей данных;

4) угрозы, связанные с человеческим фактором.

Более детально рассмотрим каждый пункт.

Угрозы, связанные с обработкой файлов.

Сложные форматы файлов (DWG, DXF, STEP, IGES и др.), с которыми работают САПР, могут привести к ряду ошибок при парсинге: например, переполнение буфера, выполнение произвольного кода и др. Так, уязвимость библиотеки «adem2d.dll» системы автоматизированного проектирования ADEM CAD/CAM/CAPP вызвана выходом операции за границы буфера в памяти. Это позволяет злоумышленнику изменить данные адресного пространства программы, что может привести к нарушению целостности пользовательских данных.

Кроме того, на этапе разработки архитектуры или концепции системы уже могут возникнуть уязвимости, такие как использование слабых протоколов аутентификации, неправильная модель управления доступом или отсутствие фильтрации.

Устаревшие или неподдерживаемые версии программ также повышают риск успешных атак. Это связано с тем, что такие программные средства уязвимы к известным эксплойтам. Более того, устаревшее программное обеспечение сложнее тестировать, исправлять, а также оно может быть несовместимо с различными файлами.

Для снижения выявленных угроз целесообразно реализовать комплекс защитных мер. Необходимо создать каталог версий САПР и сопутствующих элементов. Для предотвращения возможности наличия вредоносных программ, вшитых в обновления, необходимо проводить тесты программ в изолированной среде перед внедрением обновлений. В качестве мер несанкционированного доступа к интерфейсам, следует строить контроль доступа по принципу наименьших привилегий, а также устанавливать многофакторную аутентификацию для пользователей и администраторов. В целях снижения потерь и повышения устойчивости требуется контроль целостности файлов и регулярные аудиты изменений на уровне конфигураций и инфраструктуры.

Угрозы, связанные с вредоносным программным обеспечением.

Злоумышленники могут внедрять вредоносный код в файлы САПР. При открытии такого файла вредоносный код выполняется на компьютере

пользователя. Например, известны случаи, когда группировка Librarian Ghouls рассылает вредоносные архивы RAR с поддельными документами в формате .SCR. Если жертва открывает такой файл, то вредоносный код может быть внедрен в скрипты, макросы или другие встроенные элементы файлов САПР. Кроме самих файлов, вредоносный код может содержаться в плагинах и расширениях для САПР.

В качестве защиты против вредоносных программ, организации должны формировать комплекс мер кибербезопасности на уровне конечных точек и серверов. Здесь важную роль играет контроль запускаемых исполняем файлов. Из этого следует необходимость внедрения списка предварительно одобренных объектов (белый список). Дополнительно требуется проверка кода и способов его внедрения. Кроме того, централизованные журналы и механизмы реагирования на инциденты позволят также снизить риски внедрения вредоносных программ.

Угрозы, связанные с хранением и передачей данных:

Данный тип угроз может возникнуть в следствие незащищенного хранения файлов САПР на локальных дисках и сетевых ресурсов. В таком случае данные имеют риск стать недоступными или поврежденными в виду программных сбоев при записи или аппаратных неисправностей (отказ жёсткого диска, скачки напряжения).

Кроме того, использование сетевых ресурсов САПР вызывает угрозу несанкционированного доступа злоумышленников к данным: контроль над окружением сети хранения, использование встроенного программного обеспечения для удалённой атаки на другие узлы сети, несанкционированное подключение к каналам с подменой адресов.

Необходимо уделять особое внимание к передаче данных по незащищенным каналам связи. Данная угроза проявляется в виде физичекского подключения злоумышленника к сети или использование им уязвимостей сетевых протоколов. Например, протокол маршрутизации BGP (Border Gateway Protocol) используются для обмена информацией о маршрутах между автономными системами в интернете. Уязвимости в этих протоколах позволяют злоумышленнику перенаправлять трафик через свои системы или перехватывать данные.

Для снижения рисков, связаннх с хранением и передачей, данные в САПР должны быть зашифрованы и обеспечено надёжное резервное копирование с

шифрованием копий, хранение их в защищённых средах и регулярную проверку восстановления.

Угрозы, связанные с человеческим фактором.

Одни из самых распространенных угроз по нашему мнению. Причинами возникновения могут быть недостаточная осведомленность, приводящая к совершению ошибок при работе с данными САПР; использование слабых паролей и другие нарушение установленных политик безопасности.

Внедрение системного обучения сотрудников и повышение осведомлённость в области кибербезопасности снизит риски угроз, связанных с человеческим фактором. Следует формализовать процессы своевременной деактивации доступа и ясные политики использования внешних сервисов и носителей, так как права доступа должны соответствовать изменениям в должностях. Наконец, необходим мониторинг поведения пользователей и обнаружение подозрительных действий в сети.

В заверешение отметим, что использование систем автоматизированного проектирования требует системного подхода к информационной безопасности.

На основании анализа сформулированы ключевые направления повышения информационной безопасности при работе с САПР: управление версиями, изолированное тестирование обновлений; контроль доступа к интерфейсам на основе принципа наименьших привилегий с детальным аудитом; регулярные аудиты, мониторинг и процедура реагирования на инциденты; обучение персонала и формирование культуры безопасности; а также непрерывное повышение уровня защищённости через измеримые метрики и циклическое улучшение.

Реализация указанных мер должна проводиться с учётом соответствия международным и отраслевым стандартам (ISO/IEC 27001) и адаптации под конкретную САПР организации. Это позволит снизить вероятность киберинцидентов, минимизировать последствия атак, а также сохранить конкурентную интеллектуальную собственность.

Список литературы

1. C.news – Информационные технологии завтра. – URL: https://cnews.ru/link/n603956 (дата обращения: 04.10.2025).

2. ФСТЭК России – Федеральная служба по транспортному и экспортному контролю: информационно-поисковая система. – URL: https://bdu.fstec.ru/vul/2020-00708 (дата обращения: 04.10.2025).

3. Академия Selectel — Jбразовательное пространство. URL: https://selectel.ru/blog/vulnerabilities/ (дата обращения: 06.10.2025).

4. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования // АО «Кодекс» (дата обращения: 06.10.2025).

5. Сальников, К. А. Информационная безопасность в САПР / К. А. Сальников, Д. С. Мищенко // Молодежь и системная модернизация страны : Сборник научных статей 9-й Международной научной конференции студентов и молодых ученых. В 5-ти томах, Курск, 15–16 мая 2025 года. – Курск: ЗАО "Университетская книга", 2025. – С. 121-124.

References

1. C.news – Information Technologies of Tomorrow. URL: https://cnews.ru/link/n603956. Accessed: 4 Oct 2025.

2. FSTEC of Russia – Federal Service for Technical and Export Control: Information and Search System. URL: https://bdu.fstec.ru/vul/2020-00708. Accessed: 4 Oct 2025.

3. Selectel Academy – Educational Space. URL: https://selectel.ru/blog/vulnerabilities/. Accessed: 6 Oct 2025.

4. GOST R ISO/IEC 27001-2021. Information Technology. Security Techniques. Information Security Management Systems. Requirements. JSC "Kodeks". Accessed: 6 Oct 2025.

5. Salnikov, K. A.; Mishchenko, D. S. Information Security in CAD. In: Youth and Systemic Modernization of the Country: Proceedings of the 9th International Conference of Students and Young Scientists. In 5 volumes, Kursk, May 15–16, 2025. Kursk: JSC "University Book" (Universitetskaya kniga), 2025, P. 121–124.