УДК 004.056
DOI: 10.33764/2618-981X-2020-6-1-110-113

СОСТОЯНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ САПР

Роман Сергеевич Горохов
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант кафедры фотоники и приборостроения, тел. (999)463-43-96, e-mail: roma_gorohov2013@mail.ru

Сергей Николаевич Новиков
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, доктор технических наук, заведующий кафедрой информационной безопасности, тел. (383)343-91-11, e-mail: snovikov@ngs.ru

Проведен анализ современного состояния САПР. Дана характеристика положения передовых средств оснащения информационной безопасности САПР. Так как любая САПР является нестандартной информационной системой, то для гарантии ее безопасности требуется индивидуальный подход. Особое внимание уделяется потребности рационального сочетания криптографических и стеганографических способов защиты проектной документации от несанкционированного доступа. Опираясь на теоретические положения и практические данные, рассмотрены вопросы надежной и безопасной передачи проектной документации по волоконно-оптическим линиям связи. Сделан вывод о том, что при рассмотрении состояния информационной безопасности систем автоматизации проектирования, используемых на предприятиях с проектной документацией для классифицируемых продуктов, а также продуктов двойного назначения, должны создаваться надежные средства защиты, для чего необходимо использовать все средства, реализуемые в области информационной безопасности, включая стеганографические, криптографические и аппаратные способы ее обеспечения.

Ключевые слова: безопасность, защита, информация, криптография, стеганография.

STATE OF CAD INFORMATION SECURITY

Roman S. Gorohov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, Department of Photonics and Device Engineering, phone: (999)463-43-96, e-mail: roma_gorohov2013@mail.ru

Sergey N. Novikov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Dr. Sc., Head of Department of Information Security, phone: (383)343-91-11, e-mail: snovikov@ngs.ru

The analysis of the current state of CAD is carried out. The article describes the position of advanced CAD information security equipment. Since any CAD system is a non-standard information system, an individual approach to guarantee its security is required. Special attention is paid to the need for a rational combination of cryptographic and steganographic methods to protect project documentation from unauthorized access. Based on theoretical provisions and practical data, the issues of reliable and secure transmission of project documentation over fiber-optic communication lines are considered. It is concluded that when considering the state of information security of design automation systems used in enterprises with project documentation for classified products, as well as

dual-use products, reliable security tools should be created, for which it is necessary to use all the tools implemented in field of information security, including steganographic, cryptographic and hardware methods of ensuring it.

Key words: security, protection, information, cryptography, steganographic.

Введение

Состояние современных систем САПР позволяет решать закрытые проблемы: реализовывать финальное развитие, содержащее ряд периодов, таких как: обзор предписаний к изделию или продукту, подготовка к реализации и его созданию в трехмерной модели, изготовление документа проектирования, исследование действия разрабатываемого проекта изделия или продукта, используемого в самых разных условиях, создание и производство инструментов, и приборов, применяемых при изготовлении изделия, организация его изготовления [1–2].

Процесс автоматизирования проектных работ строится на основе совокупности автоматических процедур, а также действий систем, которые гарантируют организацию неформального представления дизайн-проекта, тем самым обеспечивая общую оценку работы данного проектного задания [3].

Превосходством разработанного программного и аппаратного обеспечения считается возможность безопасного проектирования продуктов двойного назначения. В настоящее время не существует устоявшихся способов и средств обеспечения защиты информации для секретных продуктов САПР, и изделий двойного назначения. Значимым минусом многих САПР считается дефицит возможностей предохранения от нежелательного вторжения.

Применяемые методы

Сегодня проблемы безопасности информационных систем приобретают все более серьезный характер. Если теоретический и практический опыт в области безопасности для систем «общего назначения» уже накоплен, то специальные комплексные разработки в области информационной безопасности САПР только начинаются. Следующие примеры демонстрируют важность таких разработок. LockheedMartin – это аэрокосмическая фирма США, укравшая в 1997 году сведения об устройстве самолета-невидимки и электронные чертежи. А уже в самом начале 21 века найдена вирусная программа для CAD/CAM-системы AutoCAD. В дальнейшем были выявлены довольно известные случаи подсоединения к установкам связных систем. Рассмотрим каждый подробнее.

Одним из таких случаев считается ситуация, когда в 2000 году в аэропорту германского города Франкфурта выявили подсоединение к трем основным каналам фирмы DeutscheTelekom. После этой ситуации в 2003 году был также выявлен случай, когда к оптической сети фирмы Verizone было подключено устройство, обеспечивающее прослушку этой компании. Далее похожая ситуация была зафиксирована уже в 2005 году. Все происходило на судне ВМФ США USS JimmyCarter, где были обнаружены инструменты, позволяющие осуществлять

несанкционированное присоединение к волоконным кабелям подводных лодок. Наиболее знаменитым инцидентом последнего времени являются публикация Сноуденом сведений, позволиливших подтвердить причастность National Security Agency к хищению проектных документов на засекреченные изделия, представляющие конфиденциальную информацию, которые передавались как по закрытым, так и по открытым каналам.

На сегодняшний день не существует способов, которые бы осуществляли информационную защиту проекта, а также предмета проекта в течение всего актуального цикла продукта. Те системы, которые на данный момент используются, не обеспечивают полную гарантию безопасности в случае несанкционированного доступа. Они не могут полностью учитывать некоторые функции компьютерных проектных систем, таких как, например, CAD, являющаяся открытой разрабатывающей системой [4–5].

Проведенный анализ показывает, что на данный момент требуется разработка составляющих САПР с целью осуществления информационной защиты границ коммуникаций. Если рассматривать систему CAD, то можно сказать, что данная система относится к организационно-технической, заключающейся в совокупности, с одной стороны, средств и проектов аппаратно-программного характера, а, с другой стороны – указаний экспертов, осуществляющих компьютерное планирование проектов [6–7].

Подводя итог, можно сказать, что препятствия информационной защиты САПР обладают такими отличительными чертами, которые вынуждают проводить их исследования, не затрагивая вопросы единства методов информационной защиты любых автоматизированных концепций. Несомненно, осуществление защиты проектов, которые были разработаны в сфере САПР, осуществляется тремя методами: криптографическим, стеганографическим и аппаратным [8–9].

К аппаратным методам предоставления информационной защиты, можно отнести CAD, которые содержат в себе ресурсы, обеспечивающие безопасность волоконно-оптических линий связи с целью недопущения несанкционированного доступа. Криптографические методы уделяют особое внимание обеспечению безопасности сведений, которые могут так или иначе являться государственной тайной. Поэтому считается логичным применение стеганографических методов с целью осуществления защиты проектов, изделий двойного наначения и ценных бумаг, которые могут относиться к конфиденциальной информации [10].

Заключение

При рассмотрении состояния информационной безопасности систем автоматизации для проектирования видно, что системы САПР, используемые на предприятиях с проектной документацией для классифицируемых продуктов и продуктов двойного назначения, должны иметь надежные средства защиты. Необходимо использовать все средства для защиты разработок с помощью стеганографических, криптографических и аппаратных способов обеспечения защиты информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Малюх, В. Н. Введение в современные САПР. – М.: ДМК, 2013. – 190 с.

2. Волосатова, Т. М., Чичварин, Н. В. Специфика информационной безопасности САПР // Фундаментальные проблемы создания САПР. – 2012. – № 2. – С. 89–94.

3. Кондаков, А. И. САПР технологических процессов: учебник для вузов – М.: Академия., 2008. – 267 с.

4. Волосатова, Т. М., Чичварин, Н. В. Специфика информационной безопасности САПР. – М.: МГТУ им. Н. Э. Баумана, 2013. – 75 с.

5. Медведев, И. Н., Чичварин, Н. В. Формализация построения моделей угроз информационной безопасности САПР. – М.: МГТУ им. Н. Э. Баумана, 2012. – 119 с.

6. Мишин, Е. Т. Оленин, Ю. А., Капитонов, А. А. Системы безопасности предприятия // Конверсия в машиностроении. – 1998. – № 3. – С. 31-47.

7. Ефимов, А. И. Информационная безопасность ОАО «Газпром»: проблемы гиганта // Information Security. – 2006. – №7. – С. 4 – 5.

8. Волосатова, Т. М. Исследования стеганографических методов защиты проектной документации от несанкционированного доступа // Информационные технологии. – 2014. – № 6. – С. 61-71.

9. Волосатова, Т. М., Денисов, А. В., Чичварин, Н. В. Защита проектной документации от несанкционированного доступа. – М.: МГТУ им. Н. Э. Баумана, 2012. – 144 с.

10. Волосатова, Т. М., Денисов, А.В., Чичварин, Н.В. Комбинированные методы защиты данных в САПР // Информационные технологии. – 2012.– № 4. – С. 1 – 32.