ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ САПР/PLM, ПРИМЕНЯЮЩИХ ОБЛАЧНЫЕ ТЕХНОЛОГИИ

Зорин Егор Леонидович,
***Чичварин Николай Викторович**, кандидат технических наук, доцент*

Рассмотрено состояние современных средств обеспечения информационной безопасности САПР. Показано, что поскольку САПР – весьма специфичная информационная система, необходим и специфичный подход к обеспечению ее безопасности. Он заключается в необходимости органичного включения в САПР подсистемы информационной безопасности. При этом необходим учет того, что САПР — непрерывно меняющаяся система. Кроме того показана необходимость учета специфики CALS при создании подсистемы информационной безопасности САПР. Обращается внимание на необходимость разумного сочетания криптографических и стеганографических методов защиты проектной документации от несанкционированного доступа. Рассмотрены вопросы безопасной передачи проектной документации по волоконно–оптическим линиям связи.

***Ключевые слова**: облачные технологии, безопасность, защита, информация, криптография, квантовая криптография, несанкционированный доступ, объект проектирования, проектная документация.*

INFORMATION SECURITY CAD/PLM APPLYING CLOUD TECHNOLOGY

Egor Zoryn,
***Nicolay Chichvarin**, Ph.D., Associate Professor*

The state of the modern means of information security CAD. It is shown that as CAD – very specific information system needs and specific approach to ensure its safety. He is necessary organic inclusion in CAD subsystem information security. And there must be a record of what CAD – constantly changing system. Besides the necessity of taking into account the specifics of CALS when creating information security subsystem CAD. Draws attention to the need for a judicious combination of cryptographic and steganographic methods of protection of the design documentation from unauthorized access. The problems of the safe transfer of project documentation for fiber–optic communication lines.

***Keywords**: cloud computing, security, protection, information, cryptography, quantum cryptography, unauthorized access, object design, design documentation.*

Сокращения:

АРМ – автоматизированное рабочее место	PLM – жизненный цикл изделия
ИБ – информационная безопасность	ПО – программное обеспечение
КПС – канал передачи сообщений	PLM – технологии сопровождения объекта проектирования в период жизненного цикла
НСД – несанкционированный доступ	ПС – программные средства
ОП – объект проектирования	СЗИ – система информационной безопасности
ВОЛС – волоконно – оптическая линия связи	САПР – система информационной безопасности
ОВ – оптическое волокно	CALS – сопровождение объекта проектирования в период всего жизненного цикла

Введение

Преимуществом создаваемых программно-аппаратных средств является возможность безопасного ведения проектирования изделий двойного применения. На сегодняшний день не существуют методы и средства ИБ САПР секретных изделий и изделий двойного назначения. Существенным недостатком большинства существующих САПР является отсутствие средств защиты проектной документации от несанкционированного доступа.

Собственно подключение к линиям связи выполняется достаточно просто. Вот список основных инцидентов:

- 2000 г., в аэропорту Франкфурта (Германия) обнаружено подключение к трем главным линиям компании Deutsche Telekom.

• 2003 г., на оптической сети компании Verizone обнаружено подслушивающее устройство.

• 2005 г., подводная лодка ВМФ США USS Jimmy Carter модернизирована специальным образом для установки несанкционированных подсоединений к подводным волоконным кабелям.

• Для сбора и хранения перехваченных сообщений в штате Юта (США) создан вычислительный центр на базе суперэвм с объемом внешней памяти более 100 йотабайт. Подавляющий объем данных принимается по радиоканалам, в частности, по каналам подводных лодок.

Иностранные СМИ распространяют сведения о том, что ЦРУ зафиксировало факт кражи документации на самолет, построенный по технологии STELTH.

Недавние разоблачения, сделанные агентом Сноуденом, показывают, что АНБ занимается кражей проектной документации на секретные изделия, изделия двойного применения, а также изделия, составляющие коммерческую тайну, передаваемой по открытым и закрытым каналам.

Таким образом, на данный момент существует потребность создания компоненты для обеспечения информационной безопасности линий связи. Это особенно важно, поскольку данные и ПО в облачных технологиях передаются по открытым каналам.

В работе принимается что САПР — это организационно-техническая система, состоящая из совокупности комплекса аппаратно-программных средств автоматизации проектирования и коллектива специалистов подразделений проектной организации, выполняющая автоматизированное проектирование изделия.

При этом, имеется в виду, что САПР — иерархическая система, реализующая комплексный подход к автоматизации всех уровней проектирования. Иерархия уровней проектирования является прямым следствием существования иерархии модельного представления объекта проектирования. Это создает специфические требования, предъявляемыми к САПР. Анализ доступных публикаций [3, с. 12 – 20], [5, с.150, 6, с. 103] позволяет сделать также вывод о тенденции применение CALS – технологий.

Кроме того, повышение цен на ПО САПР и усложнение дорогостоящих технических средств САПР делает средства автоматизированного проектирования недоступными для малого и среднего бизнеса, применение облачных вычислений и становится все более привлекательным PLM – технологий.

Особенно привлекательны средства облачных технологий для малых предприятий, лишенных возможности и не нуждающиеся в сложных средствах автоматизированного проектирования. Приобретая средства САПР в лизинг, организация экономит значительные средства. Поскольку применение открытых САПР, облачных технологий и PLM-технологий предполагает возможность НСД к проектной документации, проблемы обеспечения ИБ САПР становятся весьма актуальными. Многие программные средства подлежат обязательной сертификации и нуждаются в постоянном контроле специалистами по информационной безопасности. Поэтому будет справедливо считать, что вопросы ИБ САПР обладают спецификой, заставляющей рассматривать их отдельно от общих вопросов информационной безопасности остальных автоматизированных информационных систем. Очевидно, что защита проектной документации, продуцируемой в среде САПР возможна тремя методами:

- криптографическими;
- стеганографическими;
- аппаратными.

К аппаратным средствам здесь относятся и средства защиты ВОЛС от НСД. Зачастую аппаратные средства представляют собой разного рода скремблеры и устройства, маскирующие сигнал в шумах канала передачи сообщений.

Криптографические методы жестко регламентируются спецслужбами и ГОСТ, поэтому их предпочтительней применять для защиты данных, представляющих государственную тайну.

Стеганографические методы разумно использовать для обеспечения ИБ проектной документации на изделия двойного назначения и защиты документации, представляющей коммерческую тайну.

1. Постановка задачи исследований

Как показывает анализ, специфика проектной документации заключается в следующем:

• документация всегда строго структурирована в соответствии с требованиями ГОСТ;

• основные компоненты структуры – это та или иная схема (чертеж) и спецификация;

• первая компонента – всегда графическая, вторая – текстовая, изложенная в соответствии с требованиями ГОСТ языком деловой прозы.

1.1. Обзор известных методов и средств защиты проектной документации от НСД

К настоящему времени для защиты коммерческой тайны от НСД активно применяются сте-

ганографические методы. Для повышения криптостойкости предлагаются комбинированные методы, сочетающие стеганографию и применение цифровых Фурье-голограмм, искусственную дефокусировку, корреляционные (разновидность искусственной дефокусировки) методы. Для сохранения государственной тайны, а также для защиты от НСД проектной документации на изделия двойного назначения используются криптографические методы. Становятся интересными методы квантовой криптографии. Все перечисленные методы необходимо применять для защиты документации, продуцированной с применением CALS-технологий. Естественно, что защищать необходимо открытые каналы передачи сообщений.

1.2. Угрозы системам облачных вычислений и методы защиты указанных систем.

Центр обработки данных (ЦОД) представляет собой совокупность серверов, размещенных на одной площадке с целью повышения эффективности и защищенности. Защита центров обработки данных представляет собой сетевую и физическую защиту, а также отказоустойчивость и надежное электропитание. В настоящее время на рынке представлен широкий спектр решений для защиты серверов и ЦОД от различных угроз. Их объединяет ориентированность на узкий спектр решаемых задач. Однако спектр этих задач подвергся некоторому расширению вследствие постепенного вытеснения классических аппаратных систем виртуальными платформами. К известным типам угроз (сетевые атаки, уязвимости в приложениях операционных систем, вредоносное программное обеспечение) добавились сложности, связанные с контролем среды (гипервизора), трафика между гостевыми машинами и разграничением прав доступа. Расширились внутренние вопросы и политики защиты ЦОД, требования внешних регуляторов. Работа современных ЦОД в ряде отраслей требует закрытия технических вопросов, а также вопросов связанных с их безопасностью. Проектные организации подчинены ряду стандартов, выполнение которых заложено на уровне технических решений. Проникновение платформ виртуализации достигло того уровня, когда практически все проектные организации, использующие эти системы, весьма серьезно занялись вопросами усиления безопасности в них. Многие типы угроз достаточно изучены и для них разработаны средства защиты, однако их еще нужно адаптировать для использования в облаке.

1.3. Существующие угрозы системам облачных вычислений

Нет гарантий, что все ресурсы облака посчитаны и в нем нет неконтролируемых виртуальных машин, не запущено лишних процессов и не нарушена взаимная конфигурация элементов облака. Это высокоуровневый тип угроз, т.к. он связан с управляемостью облаком, как единой информационной системой и для него общую защиту нужно строить индивидуально. Для этого необходимо использовать модель управления рисками для облачных инфраструктур. В основе обеспечения физической безопасности лежит строгий контроль физического доступа к серверам и сетевой инфраструктуре. В отличие от физической безопасности, сетевая безопасность в первую очередь представляет собой построение надежной модели угроз, включающей в себя защиту от вторжений и межсетевой экран. Использование межсетевого экрана подразумевает работу фильтра, с целью разграничить внутренние сети ЦОД на подсети с разным уровнем доверия. Это могут быть отдельно серверы, доступные из Интернета или серверы из внутренних сетей. В облачных вычислениях важнейшую роль платформы выполняет технология виртуализации. Для сохранения целостности данных и обеспечения защиты рассмотрим основные известные угрозы для облачных вычислений.

1.4. Трудности при перемещении обычных серверов в «вычислительное облако»

Требования к безопасности облачных вычислений не отличаются от требований безопасности к центрам обработки данных. Однако виртуализация ЦОД и переход к облачным средам приводят к появлению новых угроз. Доступ через интернет к управлению вычислительной мощностью —одна из ключевых характеристик облачных вычислений. В большинстве традиционных ЦОД доступ инженеров к серверам контролируется на физическом уровне, в облачных средах они работают через интернет. Разграничение контроля доступа и обеспечение прозрачности изменений на системном уровне является одним из главных критериев защиты.

1.5. Динамичность виртуальных машин

Создать новую машину, остановить ее работу, запустить заново – всё это можно сделать за короткое время. Они клонируются и могут быть перемещены между физическими серверами. Данная изменчивость трудно влияет на разработку целостности системы безопасности. Однако, уязвимости операцион-

ной системы или приложений в виртуальной среде распространяются бесконтрольно и часто проявляются после произвольного промежутка времени (например, при восстановлении из резервной копии). В средах облачных вычислениях важно надежно зафиксировать состояние защиты системы, при этом это не должно зависеть от ее состояния и местоположения.

1.6 .Уязвимости внутри виртуальной среды

Серверы облачных вычислений и локальные серверы используют одни и те же операционные системы и приложения. Для облачных систем угроза удаленного взлома или заражения вредоносным ПО высока. Риск для виртуальных систем также высок. Параллельные виртуальные машины увеличивает «атакуемую поверхность». Система обнаружения и предотвращения вторжений должна быть способна обнаруживать вредоносную активность на уровне виртуальных машин, вне зависимости от их расположения в облачной среде.

1.7. Защита бездействующих виртуальных машин

Когда виртуальная машина выключена, она подвергается опасности заражения. На выключенной виртуальной машине абсолютно невозможно запустить защитное программное обеспечение, в то же время возможностей доступа к хранилищу образов виртуальных машин через сеть достаточно. В данном случае должна быть реализована защита не только внутри каждой виртуальной машины, но и на уровне гипервизора.

1.8. Защита периметра и разграничение сети

При использовании облачных вычислений периметр сети размывается или исчезает. Это приводит к тому, что защита менее защищенной части сети определяет общий уровень защищенности. Для разграничения сегментов с разными уровнями доверия в облаке виртуальные машины должны сами обеспечивать себя защитой, перемещая сетевой периметр к самой виртуальной машине. Корпоративный firewall — основной компонент для внедрения политики IT безопасности и разграничения сегментов сети, не в состоянии повлиять на серверы, размещенные в облачных средах.

2. Анализ атак на облака и решения по их устранению

2.1. Традиционные атаки на программное обеспечение

Уязвимости операционных систем, модульных компонентов, сетевых протоколов и др. — традиционные угрозы, для защиты от которых достаточно установить межсетевой экран, firewall, антивирус, IPS и другие компоненты, решающие данную проблему. При этом важно, чтобы данные средства защиты эффективно работали в условиях виртуализации.

2.2. Функциональные атаки на элементы облака

Этот тип атак связан с многослойностью облака, общим принципом безопасности. В статье об опасности облаков было предложено следующее решение: «для защиты от функциональных атак для каждой части облака необходимо использовать следующие средства защиты: для прокси – эффективную защиту от DoS-атак, для веб-сервера — контроль целостности страниц, для сервера приложений — экран уровня приложений, для СУБД — защиту от SQL-инъекций, для системы хранения данных – правильные бэкапы (резервное копирование), разграничение доступа». В отдельности каждые из этих защитных механизмов уже созданы, но они не собраны вместе для комплексной защиты облака, поэтому задачу по интеграции их в единую систему нужно решать во время создания облака.

2.3. Атаки на клиента

Большинство пользователей подключаются к облаку, используя браузер. Здесь рассматриваются такие атаки, как Cross Site Scripting, «угон» паролей, перехваты веб-сессий, «человек посредине» и многие другие. Единственная защита от данного вида атак является правильная аутентификация и использование шифрованного соединения (SSL) со взаимной аутентификацией. Однако, данные средства защиты не очень удобны и очень расточительны для создателей облаков. В этой отрасли информационной безопасности есть еще множество нерешенных задач.

2.4. Атаки на гипервизор

Гипервизор является одним из ключевых элементов виртуальной системы. Основной его функцией является разделение ресурсов между виртуальными машинами. Атака на гипервизор может привести к тому, что одна виртуальная машина сможет получить доступ к памяти и ресурсам другой. Также она сможет перехватывать сетевой трафик, отбирать физические ресурсы и даже вытеснить виртуальную машину с сервера. В качестве стандартных методов защиты рекомендуется применять специализированные продукты для виртуальных сред, интеграцию хост-серверов со службой каталога Active Directory, использование

политик сложности и устаревания паролей, а также стандартизацию процедур доступа к управляющим средствам хост-сервера, применять встроенный брандмауэр хоста виртуализации. Также возможно отключение таких часто неиспользуемых служб как, например, веб-доступ к серверу виртуализации.

2.5. Атаки на системы управления

Большое количество виртуальных машин, используемых в облаках, требует наличие систем управления, способных надежно контролировать создание, перенос и утилизацию виртуальных машин. Вмешательство в систему управления может привести к появлению виртуальных машин — невидимок, способных блокировать одни виртуальные машины и подставлять другие. Наиболее эффективные способы защиты в области безопасности облаков опубликовала организация Cloud Security Alliance (CSA). Проанализировав опубликованную компанией информацию, были предложены следующие решения.

3. Сохранность обрабатываемых данных. Шифрование данных.

Шифрование – один из самых эффективных способов защиты данных. Провайдер, предоставляющий доступ к данным должен шифровать информацию клиента, хранящуюся в ЦОД, также в случаи отсутствия необходимости, безвозвратно удалять.

3.1.Защита данных при их передаче

Зашифрованные данные при передаче должны быть доступны только после аутентификации. Данные не получится прочитать или сделать изменения, даже в случаи доступа через ненадежные узлы. Такие технологии достаточно известны, алгоритмы и надежные протоколы AES, TLS, Ipsec давно используются провайдерами. В публикации [7, с. 174] приводятся результаты исследований, проведенных авторами настоящей публикации применительно к защите САПР, применяющихся предприятиями, использующими CALS и PLM технологии.

3.2. Аутентификация

Известно, что аутентификация – защита, главным образом, паролем . Для обеспечения более высокой надежности, часто прибегают к таким средствам, как токены и сертификаты. Для прозрачного взаимодействия провайдера с системой идентификации при авторизации, также рекомендуется использовать LDAP (Lightweight Directory Access Protocol) и SAML (Security Assertion Markup Language).

3.3. Изоляция пользователей

Задача успешно решается путем использования индивидуальной виртуальной машины и виртуальной сети [8]. Виртуальные сети должны быть развернуты с применением таких технологий, как VPN (Virtual Private Network), VLAN (Virtual Local Area Network) и VPLS (Virtual Private LAN Service). Часто провайдеры изолируют данные пользователей друг от друга за счет изменения данных кода в единой программной среде. Данный подход имеет риски, связанные с опасностью найти дыру в нестандартном коде, позволяющему получить доступ к данным. В случаи возможной ошибки в коде пользователь может получить данные другого.

Облачные технологии и соответствующие решения помогают добиться как значительной экономии, так и повышения гибкости. Однако при внедрении этих технологий на предприятиях не следует оставлять без внимания традиционные процессы — их необходимо оптимизировать в расчете на новые условия. Из-за отсутствия физического доступа к серверам в публичных облачных средах вопросы безопасности становятся еще более важными, ведь в чрезвычайной ситуации не будет возможности нажать кнопку экстренного отключения.

В публичных облаках для создания новых клиентских учетных записей и облачных серверов потребуется лишь несколько минут времени и действующая кредитная карточка. Опыт показывает, что предприятиям не удается предотвращать ситуации, когда их сотрудники, к примеру, приобретают ресурсы для целей моделирования, включая их стоимость в командировочные расходы или оплачивая с помощью корпоративных кредитных карт. К сожалению, в результате реальное число облачных серверов, на которых хранятся конфиденциальные корпоративные данные, может значительно превосходить то количество, которое находится под контролем ответственных специалистов.

Поэтому гораздо безопаснее обеспечить сотрудникам проектной организации контролируемый доступ к этим ресурсам. Многие брокеры внешних и внутренних облаков предлагают широкие возможности администрирования доступа для отдельных лиц в соответствии с пользовательской, ролевой или мандантной моделью в рамках общего доступа. С одной стороны, в этом

случае предоставляются только те права, которые действительно необходимы пользователям, а с другой — повышается безопасность на предприятии, поскольку права распределяются централизованно и дифференцированно.

Такие функции предоставляют все наиболее популярные облачные брокеры, такие как vCloud Director, Amazon/ IAM, OpenStack и CloudStack. Во многих случаях возможна даже комбинация локальных и внешних ресурсов. Отказ от этих функций равносилен наличию одного общего пароля для всех сотрудников компании, работающих за общим компьютером, — очевидно, не самый благоприятный сценарий.

Поэтому создание и использование ролей, индивидуальных учетных записей или мандантов следует считать обязательным.

Независимо от того, под управлением какой операционной системы функционирует облачный сервер, доступ к нему необходимо защитить. Конечно, можно положиться на предоставленные брокером облачных сервисов случайные пароли, но обычно пользователи эти пароли либо где-нибудь записывают, либо заменяют их простыми стандартными комбинациями. Оба варианта не самые удачные. Еще один из подходов заключается в разделении внутреннего и внешнего подтверждения прав доступа (Credentials). Это можно реализовать на базе собственных серверов доступа/SSH/ RDP Proxy или с помощью специализированных коммерческих решений. При этом сотрудники указывают свой внутренний пароль для регистрации на сервере доступа, а после проверки предоставленных им прав получают доступ к облачному серверу. Таким образом, при обращении к внешним ресурсам они смогут использовать свои собственные (доменные) пароли без угрозы для безопасности.

Этот вариант привлекателен особенно в слабо защищенных средах Windows, поскольку, с точки зрения пользователей, доменные пароли пригодны для авторизации на облачных серверах, причем внешние облачные серверы не получают доступа к элементам Active Directory и их не нужно включать в домен. Периодическая смена паролей тоже значительно облегчается (а в некоторых случаях становится наконец-то возможной), поскольку внутренние и внешние процессы авторизации разделены. Как и любая другая система, облачные серверы тоже создают журнальные записи (Log Data). Однако специалисты часто забывают о том, что журнальные записи могут служить важным источником информации при проведении инженерно-технических экспертиз (особенно для динамически запускаемых и останавливаемых облачных серверов). При необходимости такой экспертизы, к примеру, в случае хакерской атаки, эти данные (при их наличии) зачастую оказываются единственной зацепкой, ведь соответствующие облачные серверы уже могут быть выведены из эксплуатации.

Поэтому сохранение важных журнальных записей (вход/выход пользователей, целостность системы, обновления) за весь срок службы облачного сервера является важной и необходимой мерой. Только сбор данных, их объединение и вывод на внешние инструменты, к примеру, на сервер Syslog, платформу безопасности с функцией проверки журналов или на систему управления событиями информационной безопасности (Security Information and Event Management, SIEM), позволят осуществить их последующий анализ. Атака на группу облачных серверов может остаться незамеченной, если атаки злоумышленника станут направляться каждый раз на новый сервер, но после вывода журнальных записей за пределы облачных серверов и выполнения их систематизации такое поведение можно будет быстро обнаружить

С точки зрения обеспечения информационной безопасности САПР/PLM, облака представляют собой лишь одну из разновидностей инфраструктурных платформ, пусть даже с высокой степенью автоматизации. Разумеется, и в системах облачных вычислений обязательно создавать процессы, которые хорошо зарекомендовали себя в традиционных физических системах. Такие основополагающие функции, как межсетевой экран, IDS/ IPS, виртуальное закрытие уязвимостей (Virtual Patching) и антивирусы, являются обязательными элементами любой концепции безопасности, будь то физические, виртуальные или облачные системы. Необходимо, чтобы все серверы из локальных, внутренних или внешних облаков были идентифицированы и интегрированы в концепцию управления безопасностью. При использовании облачных сервисов этого можно добиться посредством прямой интеграции с брокером облачных сервисов, который в любой момент может предоставить информацию о наличии различных облачных серверов. Сопоставлять вручную параметры эксплуатируемых серверов с требованиями систем безопасности в динамических средах невозможно, а при попытках такого сравнения возникают многочисленные ошибки. Но, к сожалению, в этом случае действует принцип самого слабого звена: если какой-либо облачный сервер

не интегрирован в систему управления безопасностью, то есть не защищен в достаточной мере, то для злоумышленников именно он является наиболее привлекательной мишенью. А когда информация обо всех облачных серверах предоставляется автоматически, независимо от их расположения, с помощью профилей безопасности можно оперативно вносить изменения для любого количества облачных серверов.

Вместе с тем, это позволяет централизованно контролировать изменения, производимые на облачных серверах (к примеру, в файлах или реестре). Чтобы снизить трудоемкость отслеживания таких событий, необходимо обеспечить автоматическую фильтрацию этих данных посредством специализированного ПО.

Сортировать вручную все события, к примеру, при обновлении стандартной системы Linux или Windows, невозможно. Благодаря автоматической фильтрации «положительных» событий появляется возможность подробнее изучить оставшиеся, обнаружить вероятные несанкционированные действия и отследить их [8].

Заключение

Проведенные исследования позволяют сделать следующие выводы:

1. Информационная безопасность предприятий, применяющих облачные технологии, нуждается в разработке новых надежных и недорогих средств.
2. Рекомендована и показана возможность применения стеганографических методов для защиты проектной документации и ПО, передаваемых по открытым линиям связи.

Литература:

1. Волосатова Т. М., Чичварин И. Н. Специфика информационной безопасности САПР // Известия высших учебных заведений. Сер. «Машиностроение». 2012. Спецвыпуск «Фундаментальные проблемы создания». С. 89-94.
2. Мишин Е. Т., Оленин Ю. А., Капитонов А. А. Системы безопасности предприятия – новые акценты // Конверсия в машиностроении. 1998. № 4. С. 5-6.
3. Ефимов А. И. Информационная безопасность ОАО «Газпром»: проблемы гиганта. // Information Security/ Информационная безопасность. 2006. № 5. С. 4-6.
4. Волосатова Т. М., Денисов А.В., Чичварин Н.В. Комбинированные методы защиты данных в САПР // Информационные технологии. 2012. № S5. С. 1-32.
5. Норенков И.П. Разработка систем автоматизированного проектирования. Учебник для вузов.- М.: Изд-во МГТУ им. Н. Э. Баумана, 1994. 203 с.
6. Чичварин Н. В. Экспертные компоненты САПР. М.: Машиностроение, 1991. 240 с.
7. Сопоставительный анализ областей применения характерных стеганографических алгоритмов. Труды III Всесоюзной научно-техническая конференция «Безопасные информационные технологии» / Под. ред. В. А.Матвеева. М.: МГТУ им. Н. Э. Баумана, 2012. 174 с.
8. Шнайдер У. Безопасность при использовании облачных сервисов // Журнал сетевых решений LAN. 2013. № 4. С. 72-76.
9. Зубарев И. В., Радин П. К. Основные угрозы безопасности информации в виртуальных средах и облачных платформах // Вопросы кибербезопасности. 2014. № 2 (3). С. 40-45.

References:

1. Volosatova T. M., Chichvarin I. N. Spetsifika informatsionnoy bezopasnosti SAPR , Izvestiya vysshikh uchebnykh zavedeniy. Ser. “Mashinostroenie”, 2012, Spetsvypusk «Fundamental’nye problemy sozdaniya», pp. 89-94.
2. Mishin E.T., Olenin Yu.A., Kapitonov A.A. Sistemy bezopasnosti predpriyatiya – novye aktsenty, Konversiya v mashinostroenii. 1998, N 4, C.5-6.
3. Efimov A.I. Informatsionnaya bezopasnost’ OAO «Gazprom»: problemy giganta, Information Security/ Informatsionnaya bezopasnost’, 2006, N 5, pp. 4-6.
4. Volosatova T.M., Denisov A.V., Chichvarin N.V. Kombinirovannye metody zashchity dannykh v SAPR, Informatsionnye tekhnologii, 2012, N S5, pp. 1-32.
5. Norenkov I.P. Razrabotka sistem avtomatizirovannogo proektirovaniya. Uchebnik dlya vuzov.- M.: Izd-vo MGTU im.N.E. Baumana, 1994. 203, p.
6. Chichvarin N.V. Ekspertnye komponenty SAPR. M.: Mashinostroenie, 1991. 240 p.
7. Sopostavitel’nyy analiz oblastey primeneniya kharakternykh steganograficheskikh algoritmov. Trudy III Vsesoyuznoy nauchno-tekhnicheskaya konferentsiya «Bezopasnye informatsionnye tekhnologii» / Pod. Red. V.A.Matveeva. M.: MGTU im.N.E.Baumana, 2012. 174 p.
8. Shnayder U. Bezopasnost’ pri ispol’zovanii oblachnykh servisov, Zhurnal setevykh resheniy LAN, 2013, N 4, pp. 72-76.
9. Zubarev I.V., Radin P.K. Osnovnye ugrozy bezopasnosti informatsii v virtual’nykh sredakh I oblachnykh platformakh, Voprosy kiberbezopasnosti, 2014, N 2(3), pp. 40-45.