В. ЛИМ, В. ХИМИЧ, Ю АРБУЗОВ, В. ГАЛЫГА, И. ВОЕВОДИН

Обеспечение информационной безопасности систем проектирования работ при ремонте объектов топливно-энергетического комплекса

Все опасные воздействия на системы автоматизированного проектирования строительного производства (САПР СП) при капитальном ремонте объектов топливно-энергетического комплекса (ТЭК) подразделяют на случайные и преднамеренные. Анализ опыта проектирования, изготовления и эксплуатации САПР СП показывает, что информация подвергается различным случайным воздействиям на всех этапах цикла жизни и функционирования автоматизированных систем.

Причинами случайных воздействий при эксплуатации АС могут быть: аварийные ситуации из-за стихийных бедствий и отключений электропитания; отказы и сбои аппаратуры; ошибки в программном обеспечении; ошибки в работе обслуживающего персонала и пользователей; помехи в линиях связи из-за воздействия внешней среды.

Ошибки в программном обеспечении (ПО) являются распространенным видом компьютерных нарушений. Чем выше сложность подобного ПО САПР СП, тем больше вероятность обнаружения в нем ошибок и уязвимостей. Большинство из них не представляют никакой опасности, некоторые же могут привести к серьезным последствиям, таким как получение злоумышленником контроля над сервером, неработоспособность сервера, несанкционированное использование ресурсов. Обычно подобные ошибки устраняются с помощью обновлений, регулярно выпускаемых производителем ПО. Своевременная установка таких обновлений является необходимым условием безопасности информации.

Преднамеренные угрозы связаны с целенаправленными действиями нарушителя. В качестве нарушителя может быть служащий, посетитель, конкурент, наемник и т.д. Действия нарушителя могут быть обусловлены разными мотивами: недовольством служащего своей карьерой, сугубо материальным интересом (взятка), любопытством, конкурентной борьбой, стремлением самоутвердиться любой ценой и т.п.

Наиболее распространенным и многообразным видом компьютерных нарушений является несанкционированный доступ (НСД). К угрозам НСД к защищаемой информации в САПР СП относятся угрозы доступа к информации и программному обеспечению с нарушением установленных правил разграничения доступа. Для получения НСД используются программные и аппаратные средства, входящие в состав автоматизированной системы. Угрозы НСД, которые осуществляются с использованием дополнительных, специально создаваемых для этих целей программных (программно-аппаратных) средств, рассматриваются как самостоятельный класс угроз - угроз несанкционированных программно-математических воздействий (ПМВ) на защищаемую информацию и ресурсы автоматизированной системы (АС).

По источнику проявления угрозы НСД подразделяются на: создаваемые внутренним или внешним нарушителем (физическим лицом); создаваемые аппаратной закладкой (встроенной или автономной); создаваемые вредоносными программами.

Отметим, что проявление угроз НСД в виде воздействия нарушителя на информационные потоки и базы данных возможно с автоматизированного рабочего места (АРМ) оператора системы. При использовании АРМ несколькими пользователями, авторизующимися в системе с использованием ролевой аутентификации, усложняется возможность установления факта НСД и истинного нарушителя, так как каждый из пользователей потенциально имеет доступ ко всем ресурсам АС.

Наиболее распространенными угрозами НСД в САПР СП являются: несанкционированное использование информационных ресурсов системы; хищение съемных носителей информации; получение неучтенной копии защищаемой информации; несанкционированное использование оставшейся на носителях остаточной информации после ее обработки; подключение к устройствам ПЭВМ специальной аппаратуры, с помощью которой можно регистрировать информацию; изменение конфигурации ПЭВМ и вставка постороннего устройства; ввод в систему вредоносных программных средств.

Субъектом НСД к информации может быть человек или инициированный им процесс, действия которого нарушают регламентируемые на объекте правила разграничения доступа к информации.

НСД к информации на основе преодоления программных средств разграничения доступа к ресурсам компьютера может осуществляться за счет: проникновения в систему с несанкционированными параметрами входа путем подбора пароля или обход средств защиты системы; использования низкоуровневых процессов вычислительной си-

ЛИМ Владимир Григорьевич *- кандидат технических наук, доцент Астраханского государственного университета.*
Адрес: 414000, г. Астрахань, Главпочтамт, А/Я 122
e-mail: lim@astranet.ru
ХИМИЧ Виталий Николаевич *- главный инженер ООО «Передвижная механизированная колонна № 4».*
Адрес: 117418, г. Москва, ул. Цюрупы, д. 1, стр. 6
АРБУЗОВ Юрий Алексеевич *- главный инженер ООО «Газпром трансгаз Нижний Новгород».*
Адрес: 603950, г. Нижний Новгород, ул. Звездинка, 11
ГАЛЫГА Вячеслав Станиславович *- главный механик ООО «Передвижная механизированная колонна №4».*
Адрес: 117418, г. Москва, ул. Цюрупы, д. 1, стр. 6
ВОЕВОДИН Илья Геннадьевич *- кандидат технических наук, старший преподаватель Астраханского государственного университета.*
Адрес: 414000, г. Астрахань, Главпочтамт, А/Я 124
e-mail: i-voevodin@yandex.ru

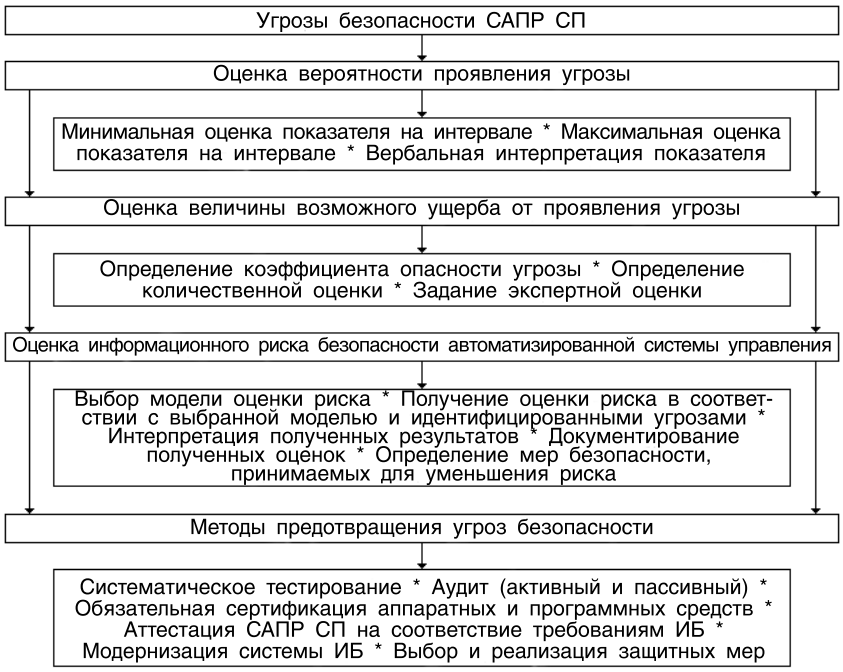

Рис. 1. *Схема оценки вероятности и величины возможного ущерба от проявления угрозы*

стемы, на которые не распространяется контроль средств защиты, например, каналов обмена информацией между процессами в операционной системе («скрытые каналы»); использования скрытых, недокументированных разработчиками возможностей программного обеспечения («люков»).

При эксплуатации ПЭВМ (АРМ) несколькими пользователями и наличии среди них возможного нарушителя опасность НСД возрастает, так как каждый из них имеет санкционированный доступ к средствам загрузки, ввода-вывода информации, что усложняет возможности по установлению факта НСД и истинного нарушителя.

Существуют также угрозы информационной безопасности (ИБ) САПР СП, которые могли быть созданы преднамеренно в ходе проектирования и разработки аппаратного и программного обеспечения в виде недекларированных возможностей операционных систем, прикладного программного обеспечения, электронного оборудования и т. п. Эти угрозы могут быть реализованы в виде специально встроенных устройств или программных закладок (ПЗ).

Включение в состав модели угроз САПР СП программных и аппаратных закладок необходимо вследствие широкого использования в составе подобных систем несертифицированных импортных технических и программных средств для хранения, обработки и передачи информации, не защищенных от утечки информации или использующих алгоритмы криптографической защиты, не соответствующие отечественным стандартам.

Обобщенная схема алгоритма оценки вероятности проявления угрозы и величины возможного ущерба от проявления угрозы представлена на **рис. 1**.

Существующее большое разнообразие угроз безопасности информации затрудняет типовой подход к их классификации. В результате в научной литературе и на практике фигурирует множество различных классификационных схем, как правило, предназначенных для различных практических целей. Отметим, что построение модели угроз ИБ является ключевым этапом создания подсистемы ИБ САПР СП [1, 2].

Построение модели угроз является одним из этапов мероприятий по обеспечению безопасности информации в САПР СП, основными из которых являются: разработка организационного, аппаратного и программного обеспечения; обеспечение ИБ при взаимодействии САПР СП с другими системами и сетями, в том числе с открытыми; обеспечение ИБ при защите от вредоносных программ; действия, связанные с модернизацией и обслуживанием САПР СП; аттестация САПР СП на соответствие требованиям ИБ и т.д.

От того, как построена модель угроз, зависит эффективность построенной с использованием этой модели системы защиты информации. Недооценка угроз приведет к повышению уязвимости системы и, в конечном счете, к реализации этих угроз, т.е. к аварийному останову системы и даже ее краху. Напротив, учет несущественных угроз приведет к усложнению алгоритмов построения системы защиты информации (СЗИ) и к ошибкам при их реализации. Переоценка угроз существенно увеличит затраты на создание СЗИ. Следовательно, построение модели угроз ИБ является ключевым этапом создания подсистемы ИБ САПР СП.

Топливно-энергетический комплекс России, определяющий в формировании экономического и научного потенциала государства и в обеспечении энергетической безопасности, всегда будет объектом для информационного воздействия со стороны ряда государств, претендующих на мировое господство, а также крупнейших мировых энергетических компаний. Чем выше будет его научно-технический потенциал, тем больше информационно-телекоммуникационных ресурсов попадет в число потенциальных целей, к которым относятся и автоматизированные системы управления. Это поднимает вопросы технической защиты информационных ресурсов ТЭК на новый уровень, от систем пассивной защиты к созданию упреждающих систем защиты.

Литература:

1. Шивдяков Л.А. Проблемы обеспечения информационной безопасности в ключевых системах информационной инфраструктуры органов государственного управления. Модель угроз безопасности информации в КСИИ // Безопасность информационных технологий. - 2009. - № 2.

2. Колотилов Ю.В., Кузнецов П.А., Лим В.Г., Климов Ю.Н. Использование методов оценки информационного риска для выбора средств защиты информации в среде САПР на предприятиях строительного комплекса // Вопросы защиты информации. - 2003. - № 3(62). - С. 50-53.