Перед лицом информационных угроз: чем вооружиться предприятию?

Т.Г. Белкин (АО "Информакустика"),
И.В. Трохалин (Группа компаний АСКОН)

Систематизированы угрозы информационной безопасности при использовании ИПИ-технологий и определены организационно-технические и инструментальные направления борьбы с ними. Наиболее подробно обсуждаются методы снижения рисков и угроз, связанных с применением прикладного ПО в составе АСУ жизненным циклом изделий.

Ключевые слова: информационная безопасность, системы управления жизненным циклом изделий, информационная поддержка процессов жизненного цикла изделий, кибербезопасность.

Современная промышленность немыслима без средств автоматизации проектирования, подготовки производства и собственно производства. В отрасли машиностроения (и особенно при производстве сложных изделий) приходится также учитывать наличие кооперационных и межведомственных связей, возникающих на всех этапах жизненного цикла продукции, необходимость участия изготовителя в послепродажном обслуживании, капитальном ремонте, модернизации изделия. И здесь уже следует говорить о программных инструментах, стандартах и технологиях для управления информацией об изделии в ходе всех этих процессов.

Начнем с терминологии. Концепция, которая объединяет принципы и технологии информационной поддержки жизненного цикла продукции на всех его стадиях, которая основана на использовании интегрированной информационной среды и обеспечивает при этом единые способы управления процессами и взаимодействия участников через электронный обмен данными, называется CALS (Continuous Acquisition and Life cycle Support) [1].

Русскоязычная формулировка этого понятия — информационная поддержка процессов жизненного цикла изделий (ИПИ), ее и будем использовать далее. Инструментарием ИПИ являются такие классы программных средств, как: автоматизированные системы конструкторского и технологического проектирования (CAE/CAD/CAM); программные средства управления данными об изделии или изделиях (PDM); автоматизированные системы планирования и управления производством и предприятием (MRP/ERP); программно-методические средства анализа логистической поддержки и ведения баз данных по результатам такого анализа (LSA/LSAR) и др.

Совокупность технических и программных средств ИПИ, информации, а также пользователей в контуре обработки информации, объединяющем всех участников разработки, изготовления и эксплуатации изделия, будем называть АСУ ЖЦИ.

В основе ИПИ лежит понятие интегрированной информационной среды (ИИС) предприятия или группы предприятий, задействованных в процессах ЖЦИ. Терминологический словарь [2] определяет ИИС как совокупность распределенных баз данных, содержащих сведения об изделиях, производственной среде, ресурсах и процессах предприятия, обеспечивающую корректность, актуальность, сохранность и доступность данных тем субъектам производственно-хозяйственной деятельности, осуществляющим жизненный цикл, кому это необходимо и разрешено.

Здесь реализуется главный принцип ИПИ: однажды возникшая информация сохраняется в ИИС и становится доступной всем участникам этого и других этапов в соответствии с имеющимися у них правами доступа.

Таким образом, ИПИ-технологии всегда связаны с коллективным доступом к информации большого числа пользователей, принадлежащих не только к разным подразделениям одного предприятия, но и к разным предприятиям. И именно в информационной доступности кроются основные эффекты от использования ИПИ-технологий. Однако, если речь идет об информации ограниченного распространения, относящейся к коммерческой, служебной или государственной тайне, в действие вступает ряд ограничений. Во-первых, необходимо максимально снизить риски несанкционированного доступа к информации. Во-вторых, производственные и логистические процессы, зависящие от такой информации, должны быть непрерывными, соответственно нужно обеспечить целостность и доступность этой информации. В-третьих, все происходящее должно соответствовать законодательству и нормативным требованиям в области защиты информации[1] в части

[1] В соответствии с ГОСТ Р 51583-2014 «целью создания системы защиты информации является обеспечение защиты информации от неправомерного доступа, уничтожения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации, соблюдение конфиденциальности информации ограниченного доступа, реализация права на доступ к информации».

обеспечения заданных руководящими документами показателей защищенности информации. Все эти ограничения требуют комплекса средств и мер защиты как на уровне интегрированного взаимодействия предприятий между собой, так и внутри отдельного предприятия с сохранением всех тех эффектов ИПИ-технологий, ради которых они и внедряются.

Здесь-то промышленность и встречает множество вызовов. А гарантированно рабочих, стандартных подходов в этой области попросту нет.

Авторы приняли участие в проведении ряда НИР и ОКР, в ходе которых были систематизированы угрозы информационной безопасности (ИБ) при использовании ИПИ-технологий и определены направления борьбы с ними как организационные и технические, так и на уровне проработки развития инструментов ИПИ. Рассмотрим наиболее общие положения накопленного опыта по проблематике ИБ в ИПИ-технологиях: угрозы, риски и способы борьбы с ними. Конечно, перечень угроз и мер для их пресечения слишком широк для освещения в пределах одной статьи. Поэтому сделаем акцент на наименее проработанной области — методах снижения рисков и угроз, связанных с применением прикладного ПО (ППО) в составе АСУ ЖЦИ, и предложим к обсуждению подходы к их нейтрализации.

Угрозы ИБ: проблематика и решения

Говоря о комплексной модели угроз, которые могут возникнуть при обработке информации в АСУ ЖЦИ стратегического назначения, целесообразно выделить главные из них, связанные с применением ППО. Итак...

Утечка защищаемой информации

Реализацией такой угрозы считается событие, при котором случается несанкционированное ознакомление со сведениями ограниченного доступа через носители информации и/или средства вычислительной техники защищаемой АСУ как штатными инструментами АСУ, так с помощью подключения неразрешенной техники к защищаемой АСУ.

Поскольку этот вид угроз рассматривается в контексте формирования единого информационного пространства для всех участников управления ЖЦИ, то применение наложенных средств защиты информации не может обеспечить в полной мере сохранность данных от несанкционированного ознакомления. К числу лиц, чей доступ должен быть ограничен, относятся в этом случае также и штатные пользователи АСУ: они могут работать с системой, но внутри PDM им должны быть доступны только отдельные объекты. То же самое касается и интеграционных механизмов: обмен данными в рамках АСУ ЖЦИ осуществляется по технологиям межпрограммного взаимодействия между различными прикладными программами и в большинстве случаев не может быть проконтролирован наложенными средствами (только ППО может обеспечить дискреционный и мандатный механизмы управления доступа к объектам, имеющим отличную от файлов и сокетов природу).

Источниками угроз утечки информации в АСУ ЖЦИ могут быть следующие уязвимости прикладного ПО:

— отсутствие или несовершенство (слабость, наличие возможностей обхода) механизмов разграничения доступа, встроенных в прикладное программное обеспечение;

— избыточная сложность механизмов защиты, их сильные отличия или даже несовместимость между различными программными комплексами в АСУ, что приводит к ошибкам настройки или эксплуатации;

— низкий уровень документирования (отсутствие исходных данных для проектирования в части ИБ или наличие недокументированных слабостей, уязвимостей), что не позволяет учесть эти особенности прикладного ПО при проектировании АСУ в защищенном исполнении (АСУЗИ);

— отсутствие унифицированных интерфейсов безопасности информации для прикладного ПО (каждый разработчик реализует некий минимум функциональности безопасности, исходя из своих соображений, но при этом интеграция таких комплексов между собой при проектировании АСУЗИ крайне затруднительна).

К утечке информации могут также привести и косвенные факторы, связанные с ППО. Так, например, сложность прикладных программных комплексов и необходимость высокой квалификации для учета всех особенностей ППО при проектировании АСУЗИ создает предпосылки возникновения брешей в безопасности за счет ошибок в проектировании АСУЗИ, связанных с отсутствием знаний о методах и способах применения ППО в АСУЗИ. В данном случае фактором угрозы является сложность настроек комплекса вне зависимости от того, какие он имеет уязвимости в программном коде. Сама по себе технология применения при огромном числе настроек, в том числе и по ограничению доступа, создает предпосылки к тому, что никто кроме разработчика ППО толком не знает, что именно происходит с защищаемой информацией при внедрении ПО.

Несанкционированная модификация защищаемой информации

Модификация данных в системе происходит в нарушение установленных правил обработки — причем независимо от мотивов нарушителя. Определяющим признаком данного вида угрозы является нарушение форматов и смысловых признаков целостности документов, информационных массивов, информационных объектов, например, внесение умышленных искажений в числовые параметры или несанкционированное изменение статусов электронных документов или изменение маршрутов движения документов.

Источниками таких угроз могут быть:

— наличие ошибок в программном коде, которые приводят к возможности умышленного воздействия или неумышленной модификации (искажения данных с сохранением смысловой части в семантически приемлемом диапазоне);

— наличие умышленных закладок в программном коде, которые приводят к возможности умышленного воздействия или неумышленной модификации;

— сложность настройки комплекса или низкое качество документирования, которое приводит к ошибкам настройки или эксплуатации, вследствие которых могут быть совершены несанкционированные модификации защищаемых данных.

Нарушение целостности защищаемой информации

Здесь искажение значимой информации происходит с потерей смысловой части, то есть приведение в нечитаемый вид отдельных документов, чертежей или полное разрушение реквизитной части электронного документа. К возникновению такой угрозы ведут те же уязвимости прикладного ПО, которые являются источниками несанкционированной модификации.

Нарушение доступности защищаемой информации

Целостность защищаемых ресурсов автоматизированной системы сохраняется, но штатные пользователи теряют возможность доступа к этим ресурсам в регламентированном режиме.

Причиной могут стать все вышеперечисленные уязвимости ППО и факторы, связанные с его использованием, так как основная масса угроз такого характера может быть реализована путем умышленного или непреднамеренного воздействия на серверную или клиентскую часть ППО без воздействия на хранилища защищаемой информации. В этом случае критичным является то, что несмотря на сохранение самих данных в целостности, нарушается работа АСУ, и тем самым наносится серьезный ущерб жизненному циклу изделия. Помимо классических угроз ИБ крайне важно акцентировать внимание руководителей на рисках, связанных с применением средств автоматизации. Большая часть этих рисков может быть сформулирована как «риск зависимости от информационных технологий».

Нарушение доступности защищаемой информации при ее долговременном хранении

В современных условиях, когда государственный оборонный заказ преимущественно переходит на серийное изготовление военной и специальной техники, на первый план выходят вопросы, связанные с долговременной доступностью архивов КД, ТД, ЭД и другой документации на изделия военного и двойного назначения. Спроектированные изделия должны производиться в соответствии с заложенной в архив документацией. Доступ к этой документации должен быть обеспечен не только на данный момент, но и в долговременной перспективе. При этом достижение показателей обороноспособности государства, технологической независимости от внутренних стрессов и иностранного влияния во многом зависит от возможности своевременно и бесперебойно осуществлять изготовление ВВСТ по документации, находящейся в архивах предприятий. Обновление версий ПО всех компонентов АСУ ЖЦИ приводит к двум наиболее важным и заметным технологическим рискам: утрата поддержки форматов данных и утрата совместимости ПО новых версий различных производителей. Большинство ИТ-специалистов сосредоточены на поддержании в актуальном состоянии ИТ-среды, обеспечивая тем самым поддержку актуальных форматов и совместимости всех программных систем в текущий момент времени. Но решение этой задачи зачастую несовместимо с решением задачи поддержки доступности ранее сформированных массивов документации и возможности работы с ними (корректировки КД, доработки ТД для новых условий модернизируемого производства).

Риски отказа в предоставлении лицензий на ПО

Отказ в обновлении, техподдержке и т.д. в связи с санкциями или другими обстоятельствами международного характера. Освоение, апробация, внедрение и получение максимального эффекта от использования сложного ПО для реализации ИПИ — это длительный цикл, который связан с масштабными изменениями как технической инфраструктуры, так и с обучением персонала предприятия и создания определенных процедур создания продукции. Применение любого сложного инженерного ПО создает риск зависимости жизненного цикла создаваемых изделий от этого ПО. И отказ в предоставлении или продлении лицензий представляет собой серьезную проблему, ведь возможно потребуется быстро переходить на другие программные средства. В настоящее время этот риск в основном характерен для импортного ПО в связи с запретом иностранных государств производить его поставку на отдельные отечественные предприятия. Но следует отметить, что такой риск актуален и для отдельных отечественных поставщиков из-за того, что их рыночная устойчивость может быть недостаточной для противостояния затяжным экономическим спадам.

Риски существенного изменения требований к среде окружения

Изменяются требования к инфраструктуре, общесистемному ПО, средствам вычислительной техники. Обновление прикладного ПО зачастую влечет за собой увеличение требований к производительности вычислительной техники. Иногда такие требования носят характер не только количественных изменений, но и качественного прорыва, требующего замены дорогостоящих серверов или прокладки новой, более скоростной структурированной кабельной сети и обновления сетевого оборудования ее ядра. Но наиболее опасной в условиях санкций может быть необходимость перехода на новые версии общесистемного ПО (ОС, СУБД), которые могут стать недоступными для предприятий в силу санкционных или других ограничений.

Риски невыполнения функциональных требований заказчика

Обеспечение конкретных функциональных требований (в том числе требований к поддержке отраслевых типовых надстроек, необходимых конкретному

предприятию, интегрированным функциям защиты информации, требованиям к наличию сертификата на отсутствие недокументированных возможностей или ведомственного разрешения на применение) может стать препятствием к продлению лицензий на уже внедренные системы или закупке нового ПО.

Риски низкого уровня сервисов сопровождения и модернизации ПО

Одним из наиболее опасных рисков является падение уровня сервиса доработки и сопровождения ПО. Жизненный цикл сложной информационной системы длится не менее семи лет, а для получения пика эффективности автоматизации планирование должно быть не менее чем на 10 лет. Не все компании, производящие прикладное или общесистемное ПО, могут гарантировать соответствующий уровень сервиса на протяжении указанных периодов времени. И в данной ситуации очевидно, что это область регулирования государства или госкорпораций, так как подобного рода сроки гарантий часто не могут быть указаны в договорах на закупку ПО для нужд предприятия.

Риски отсутствия методологии внедрения

Успешное внедрение инженерного ПО требует в обязательном порядке проработки методологии внедрения. Это сценарии применения ПО с учетом его совместимости и взаимодействия с другими компонентами информационной системы, а также с учетом требований к модернизации инфраструктуры и ИБ. Эта задача может быть эффективно решена только при участии разработчика ПО и наличии типовых методик внедрения, которые содержат описание типовых сценариев применения ПО для их адаптации к бизнес-процессу конкретного заказчика, а также конкретные числовые показатели по требованиям к инфраструктуре, чтобы их можно было учесть при развертывании комплекса. Все это требует соответствующей инфраструктуры у поставщика ПО — начиная со службы внедрения и заканчивая требованиями к персоналу компании, осуществляющей внедрение (включая требования режимного характера).

Как справиться с угрозами и рисками?

Борьба с угрозами несанкционированного доступа и модификации, нарушения целостности и доступности информации может стать успешной, если следовать двум направлениям.

1. Обеспечение доверия к программным средствам ИПИ.

В отношении ПО от некоторых компаний-разработчиков (преимущественно зарубежных) указанные угрозы и риски являются крайне актуальными и зачастую, в силу позиции вендоров, не могут быть никак устранены с их помощью. Наиболее распространенными примерами является неготовность предоставления исходных текстов и документирования внутренних процедур обработки информации.

Как правило, позиция таких разработчиков понятна, — они руководствуются соображениями сохранности интеллектуальной собственности. Тем не менее такая ситуация сильно снижает уровень доверия к ПО для ИПИ-технологий, хотя и не является блокирующим препятствием к применению такого ПО.

Существуют методы оценки рисков, связанных с наличием ошибок или даже закладок в импортном ПО, и при соответствующей проработке контрмер эти риски могут быть сведены к допустимым границам. Обеспечение доверия к ПО требует от разработчика значительных усилий. Ведь это не только раскрытие исходных кодов, но и существенные вложения в документирование внутренних процедур обработки информации, поддержку отдельной ветки разработки ПО, встраивание в ПО новых функций защиты информации и модификация существующих, сопровождение экспертизы новых версий ПО (сроки действия сертификатов на соответствие требованиям безопасности информации ограничены тремя годами). При этом такая позиция разработчика обеспечивает не только формальную сторону доверия к ПО в виде сертификата регулятора, но и гарантию того, что все механизмы были проверены на корректность работы в тех условиях применения, для которых они предназначены. То есть проверке подлежат не только отдельные функции ПО, а вся совокупность механизмов, которые вместе со средой функционирования данного ПО обеспечивают соответствие требованиям по защите информации в АСУ определенного класса защищенности. Например, если сертификация проводится на соответствие техническим условиям, то в них прописываются не только функции по защите информации, встроенные в объект оценки, но и ограничения на эксплуатацию этих механизмов, при которых будут обеспечиваться требования к защите информации для определенного класса защищенности АСУ. А аккредитованная испытательная лаборатория проводит испытания ПО, функционирующего в предусмотренной техническими условиями среде. Такой подход позволяет значительно снизить риски неправильного проектирования АСУ, в рамках которой будет функционировать данное прикладное ПО.

2. Системный подход к проектированию и вводу в действие АСУ.

Эффективные методы и средства защиты информации не могут быть отдельной «надстройкой» над архитектурой АСУ ЖЦИ. Функции защиты информации должны быть плотно вплетены в прикладные процессы деятельности в АСУ ЖЦИ (процессы конструирования, согласования документов, обмена данными между подразделениями и предприятиями и т.д.). Поэтому АСУ, ее структура и функции, процессы деятельности в ней в идеале должны проектироваться изначально с учетом требований по защите информации. Конечно, распространенной практикой является решение вопросов защиты информации для уже существующих, функционирующих АСУ ЖЦИ, но и в этом случае необходимо подходить к процессу как к развитию АСУ со всеми обязательными для такого подхода стадиями.

1. Должна быть выделена междисциплинарная команда проекта (специалисты по ИТ и ИБ, эксперты по предметным областям автоматизации), которая будет проектировать и вводить в действие АСУ. Команда должна пройти вводные курсы обучения по всем выбранным для внедрения компонентам (ПО, элементы инфраструктуры), чтобы понимать границы возможностей их адаптации к специфике условий применения.

2. Если нет уверенности в том, что междисциплинарная команда, набранная из специалистов предприятия, имеет достаточный опыт в реализации масштабных проектов как по внедрению ИПИ-технологий, так и по выстраиванию системы защиты информации, то лучше обратиться к внешним компаниям-интеграторам в области ИПИ и ИБ.

3. Необходим полноценный этап проектирования АСУ (или ее развития), в ходе которого вырабатываются проектные решения по следующим направлениям:

а) выполнение нормативных требований по защите информации (функциями ПО, организационными мерами, инфраструктурными решениями);

б) технология обработки информации (обеспечивающая, с одной стороны, выполнение прикладных требований по управлению данными об изделии, с другой,— выполнение требований по защите информации). Одним из актуальных аспектов технологии обработки информации является вопрос управления потоками информации с различным уровнем конфиденциальности;

в) архитектура АСУ в защищенном исполнении (распределение узлов и подсетей, доменная структура и доверительные отношения между доменами, межсетевые экраны, решения по виртуализации и т. п.)

4. Должна быть готовность при необходимости проводить реинжиниринг отдельных прикладных процессов в АСУ (то есть их существенную реорганизацию) для того, чтобы меры по защите информации были эффективными, а не формальными. Может потребоваться ввести новые роли в АСУ или даже новые должности в организационную структуру и увязать их действия с другими участниками бизнес-процессов. В других случаях может потребоваться организация новых процессов, которые ранее не выполнялись.

5. Сдаче АСУ в постоянную эксплуатацию должны предшествовать испытания и опытная эксплуатация, в ходе которых проектные решения проверяются в близких к «боевым» условиях. Отсутствие этого этапа или недостаточное внимание к его результатам может привести к существенным потерям для предприятия на начальном этапе постоянной эксплуатации в связи с нарушением непрерывности основных процессов, выполняемых в рамках АСУ ЖЦИ.

Касательно «рисков зависимости от информационных технологий», перечисленных выше (риски отказа в предоставлении лицензий, изменения требований к инфраструктуре, невыполнения функциональных требований, низкого уровня сервиса сопровождения), то следует отметить необходимость прогнозирования при выборе программных средств ИПИ взаимоотношений с поставщиками ПО в долгосрочном периоде, с учетом реальной длительности жизненного цикла АСУ, который может составлять ⩾7...10 лет. Нужно учитывать устойчивость бизнеса производителя ПО, охват рынка, темпы развития ПО, наличие в портфолио проектов на предприятиях с похожей спецификой, число крупных клиентов, наличие разветвленной сети представительств, особенно в регионах, где расположены предприятия и их филиалы.

Список литературы

1. *Судов Е.В., Левин А.И.* Концепция развития CALS-технологий в промышленности России. НИЦ CALS-технологий «Прикладная логистика». М. 2002.
2. *Карташев А.В.* Проблемные вопросы интегрированной логистической поддержки жизненного цикла продукции // Материалы 3-й международной научно-практич. конференции "Методология управления высокотехнологическими предприятиями". М.: МТУ им.Н.Э.Баумана, 2008.

Трохалин Иван Вячеславович *– руководитель дивизиона PLM группы компаний АСКОН,*
Белкин Тимур Григорьевич *– директор департамента проектов системной интеграции АО "Информакустика".*
Контактный телефон +7 (495) 783-25-59

Связанные одной целью: новые элементы российской PLM-платформы на форуме «РазвИТие 2017»

27 сентября 2017 г. в Москве в третий раз пройдет форум «РазвИТие. Российские технологии для инженеров», организованный независимым консорциумом отечественных ИТ-разработчиков — компаниями АСКОН, НТЦ «АПМ», ТЕСИС, ADEM и ЭРЕМЕКС. Вот уже несколько лет консорциум выступает локомотивом развития российской PLM-платформы. В этом году разработчики представят предприятиям новые элементы концепции цифрового производства, реализованные на базе российского ПО.

Участники консорциума расскажут о стратегии развития PLM-решения — о том, что было реализовано и о планах на ближайшее будущее. Участники форума «РазвИТие» смогут в подробностях рассмотреть устройство «цифрового предприятия». В этом году вместо привычных секций гостей форума ждет «Конструкторская служба», «Технологическая служба» и «Служба производства и сервиса». Разработчики и их заказчики покажут, как продукты членов консорциума интегрированы в тот или иной этап жизненного цикла изделия и как тесное взаимодействие этих продуктов помогает решать междисциплинарные задачи.

Http://plmrussia.ru