Перед лицом информационных угроз: чем вооружиться предприятию?

Информационная безопасность в системах управления жизненным циклом изделий

Тимур Белкин,

директор департамента проектов системной интеграции ОАО «Информакустика»

Иван Трохалин,

руководитель дивизиона PLM компании АСКОН

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.

Для начала разберемся в 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) *(2)*. 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 персонала и инструментальных средств ИПИ в рамках конкретного предприятия будем называть АСУ ЖЦИ.

Библиография

1. *Р 50.1.031-2001. Информационные технологии поддержки жизненного цикла продукции. Терминологический словарь. Ч.1. Стадии жизненного цикла продукции: Рекомендации по стандартизации. — М.: Госстандарт России, 2001.*
2. *Концепция развития CALS-технологий в промышленности России / НИЦ CALS-технологий «Прикладная логистика»; Е.В. Судов, А.И. Левин. — М., 2002.*

В основе ИПИ лежит понятие интегрированной информационной среды (ИИС) предприятия или группы предприятий, задействованных в процессах ЖЦИ. Терминологический словарь *(1)* 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, разумеется, в соответствии с имеющимися у них правами доступа.

Таким образом, ИПИ-технологии всегда связаны с коллективным доступом к информации большого количества 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 этой информации. В-третьих, все происходящее должно соответствовать законодательству и нормативным требованиям в области защиты информации. Все эти ограничения требуют комплекса средств и мер защиты как на уровне интегрированного взаимодействия предприятий между собой, так и внутри отдельного предприятия, конечно, с сохранением всех тех эффектов ИПИ-технологий, ради которых они, собственно, и внедряются. Здесь-то промышленность и встречает множество вызовов. А гарантировано рабочих, стандартных подходов в этой области попросту нет.

Авторы этого материала приняли участие в проведении ряда НИР и ОКР, в ходе которых были систематизированы угрозы информационной безопасности при использовании ИПИ-технологий и определены направления борьбы с ними — как организационные и технические, так и на уровне проработки развития инструментов ИПИ. Мы выносим на суд читателя наиболее общие положения накопленного опыта по проблематике инфобезопасности 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 мы сделаем акцент на наименее проработанной области — методах снижения рисков и угроз, связанных с применением прикладного ПО в составе АСУ ЖЦИ, и предложим к обсуждению подходы к их нейтрализации.

Угрозы инфобезопасности: проблематика и решения

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

Кратко о системе защиты информации

В соответствии с ГОСТ 51583 «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».

Утечка защищаемой информации

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

Поскольку мы рассматриваем этот вид угроз 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 АС: 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 прикладное ПО может обеспечить дискреционный и мандатный механизмы управления доступа к объектам, имеющим отличную от файлов и сокетов природу).

Источниками угроз утечки информации в АСУ ЦЖИ 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 АС, что приводит к ошибкам настройки или эксплуатации;
- низкий уровень документирования (отсутствие исходных данных для проектирования в части инфобезопасности или наличие недокументированных слабостей, уязвимостей), что не позволяет учесть эти особенности прикладного ПО при проектировании АС в защищенном исполнении (АСЗИ);
- отсутствие унифицированных интерфейсов безопасности информации для прикладного ПО (каждый разработчик реализует некий минимум функционала безопасности исходя из своих соображений, но при этом интеграция таких комплексов между собой при проектировании АСЗИ крайне затруднительна).

К утечке информации могут также привести и косвенные факторы, связанные с прикладным ПО. Так, например, сложность прикладных программных комплексов и необходимость высокой квалификации для учета всех особенностей прикладного ПО (ППО) при проектировании АСЗИ создает предпосылки возникновения брешей в безопасности за счет ошибок в проектировании АСЗИ, связанных с отсутствием знаний о методах и способах применения ППО в АСЗИ. 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 количестве 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 программного обеспечения.

Несанкционированная модификация защищаемой информации

Что происходит? Модификация данных в системе происходит в нарушение установленных правил обработки — причем независимо от мотивов нарушителя. Определяющим признаком данного вида угрозы является сохранение 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

Что происходит? 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, что являются источниками несанкционированной модификации.

Нарушение доступности защищаемой информации

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

Роль могут сыграть все вышеперечисленные уязвимости прикладного ПО 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 АС, и тем самым наносится очень серьезный ущерб жизненному циклу изделия.

Помимо классических угроз информационной безопасности мы считаем крайне важным акцентировать внимание руководителей на следующих рисках, связанных с применением средств автоматизации. Большая часть этих рисков может быть сформулирована как «риск зависимости от информационных технологий».

Риски отказа в предоставлении лицензий на ПО

Что происходит? 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.

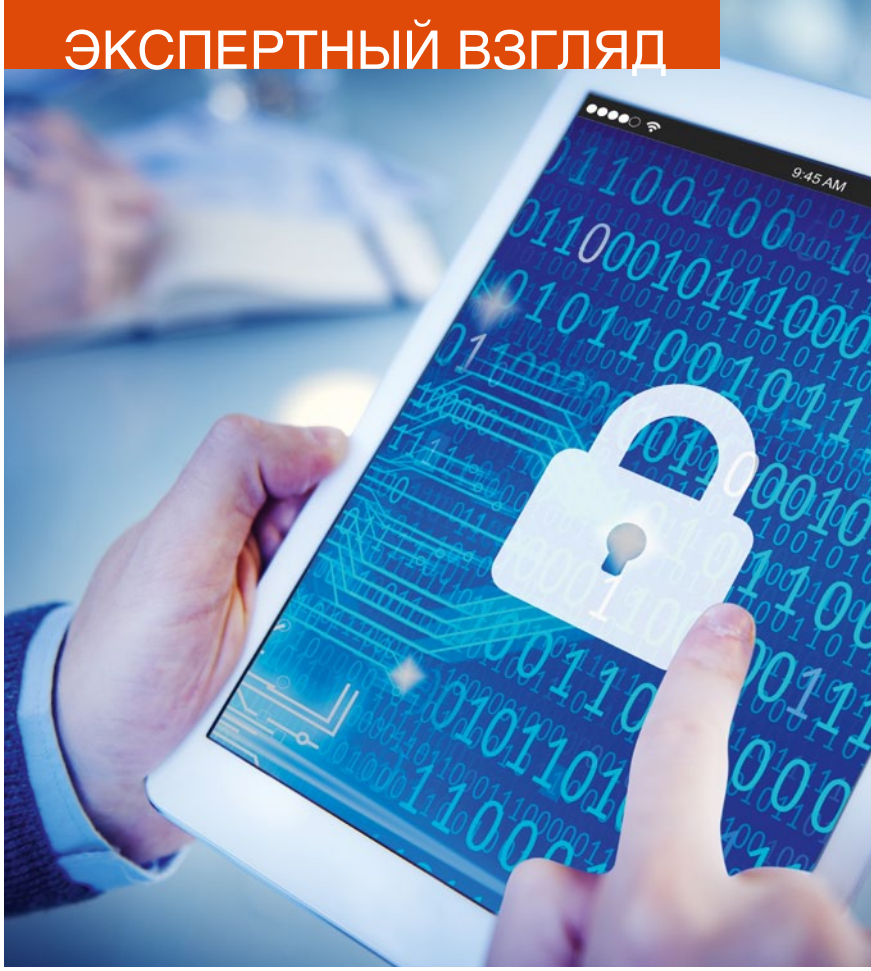
Риски существенного изменения требований к среде окружения

Что происходит? Изменяются требования к инфраструктуре, общесистемному ПО, средствам вычислительной техники.

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

Риски невыполнения функциональных требований заказчика

Что происходит? 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 НДВ 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 программного обеспечения

Что происходит? 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 десять 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 как минимум госкорпораций, так как подобного рода сроки гарантий часто не могут быть указаны в договорах на закупку ПО для нужд предприятия.

Риски отсутствия методологии внедрения

Что происходит? 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 информационной безопасности. 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 софта. 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 АС 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 АС. А аккредитованная испытательная лаборатория проводит испытания ПО, функционирующего в предусмотренной техническими условиями среде. Такой подход позволяет значительно снизить риски неправильного проектирования АС, в рамках которой будет функционировать данное прикладное ПО. (*См. Кейс № 1*)

2. Системный подход к проектированию и вводу в действие АС

Эффективные методы и средства защиты информации не могут быть отдельной «надстройкой» над ар-

Из опыта авторов

1 Кейс первый — о завершении сертификации PDM-системы

Группа компаний АСКОН совместно с ФГУП «РФЯЦ-ВНИИЭФ», ЗАО «Информакустика» и ОАО «НПО «Эшелон»» провели работы по подготовке и проведению сертификационных испытаний PDM-системы ЛОЦМАН:PLM на соответствие РД НДВ по 2-му уровню контроля, а также на соответствие техническим условиям в качестве программного средства защиты информации в АСЗИ класса до 1Б включительно. Согласно техническим условиям программное изделие предполагает обязательное наличие в среде функционирования программного средства защиты информации от несанкционированного доступа SecretNet. Функциями защиты информации, встроенными в PDM-систему и заявленными в технических условиях, являются идентификация пользователей, контроль доступа к защищаемой информации на основе матрицы доступа, регистрация событий. Разделение потоков информации различного уровня конфиденциальности производится на уровне баз данных, при этом доступ к базам данных с различным уровнем конфиденциальности может происходить как с различных рабочих мест, так и с одного и посредством одного клиентского приложения.

2 Кейс второй — о междисциплинарной команде проекта

В команду проекта по созданию АСУ ЖЦИ изначально не были включены сотрудники службы безопасности. В проекте сложилась ситуация, когда потребовалось согласование решений по инфобезопасности. Служба безопасности заняла формальную позицию: «Предоставьте полное описание технологии обработки информации, согласовывать («подписываться под») отдельные решения не готовы». Таким образом, образовался замкнутый круг, а точнее «хоровод» из «АСУшников» и «безопасников»: первым требуется согласование отдельных допущений для формирования проекта АСУ ЖЦИ, а вторым — проект АСУ ЖЦИ в конечном виде, чтобы дать по нему свой вердикт о соответствии требованиям по защите информации. Избежать этого можно общим целеполаганием внутри единой междисциплинарной команды проекта.

3 Кейс третий — о мандатном принципе контроля доступа

Задача управления потоками информации различного уровня конфиденциальности возникает при следующих условиях:

- обрабатываемая информация об изделиях имеет различные категории, в зависимости от которых устанавливаются правила доступа и обработки;
- информация различных категорий задействована в сквозных цепочках процессов жизненного цикла изделия. Категории информации, требующие особых режимов доступа и обработки, не могут быть изолированы на уровне рабочих мест специалистов (то есть невозможно выделить группу рабочих мест для работы с информацией данной категории). Иначе будут потеряны основные эффекты от использования ИПИ-технологий.

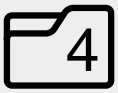
Традиционным способом решения этой задачи является применение наложенных СрЗИ, в которых реализованы механизмы управления потоками на уровне файлов. Главное ограничение такого подхода связано с тем, что все современные PDM-системы, являющиеся системообразующим элементом ИПИ-технологий, основаны на хранении информации об изделиях в виде информационных объектов в базах данных, на содержание которых контроль со стороны наложенных СрЗИ не распространяется. А наложенные СрЗИ контролируют потоки только на уровне файловых операций. В результате управление потоками при использовании наложенных СрЗИ может быть организовано только на уровне баз данных в целом (то есть информация разных категорий должна храниться в разных БД). Зачастую это приводит к дублированию инфраструктуры (серверы БД и приложений, рабочие места пользователей), усложнению технологии обработки информации для конечных пользователей и администраторов. Вариант реализации управления потоками на этом уровне, с некоторыми усовершенствованиями, в частности позволяющими клиентскому приложению PDM обращаться к БД разного уровня конфиденциальности, в настоящее время проходит финальный этап сертификации ФСТЭК по результатам работы кооперации в составе Группа компаний АСКОН, ФГУП «РФЯЦ-ВНИИЭФ», ЗАО «Информакустика» и ЗАО «НПО «Эшелон».

Следующим логичным шагом, позволяющим снять указанное выше ограничение, является встраивание механизмов управления потоками (а именно иерархического мандатного принципа контроля доступа) в PDM-систему, чтобы категорирование информации распространялось не только на файлы, но и на информационные объекты в БД. Это не отменяет использования наложенных СрЗИ, так как PDM-система по-прежнему управляет файлами, выгружая их для работы с программами-инструментами (например, CAD) на файловые ресурсы. Во всех существующих СрЗИ реализована сеансная модель управления потоками. Это значит, что для изменения категории конфиденциальности информации (файлов), с которой работает пользователь, ему необходимо как минимум выйти из программы и запустить ее заново в сеансе с другой категорией конфиденциальности, а как максимум, выйти из текущего сеанса операционной системы, перезагрузить компьютер и войти в систему с указанием другой категории конфиденциальности. При работе в PDM-системе такой подход приводит к потере эффектов от автоматизации, так как пользователи вынуждены постоянно «скакать» между сеансами, теряя текущий контекст проектирования. Вторая проблема — это правила разграничения доступа, применяемые для иерархического мандатного принципа контроля доступа (так называемая модель Белла-Лападулы), а именно невозможность чтения информации с более высокой категорией конфиденциальности, чем категория допуска (сеанса) пользователя и невозможность записи в информационные ресурсы с более низкой категорией, чем категория допуска пользователя. Это накладывает существенные ограничения на работу с агрегированными документами (состоящими из нескольких файлов), каковыми являются, например, электронные модели сборочных единиц, разрабатываемые в CAD-системах, и ассоциативными связями между компонентами в них.

Для поиска путей оптимальной реализации встроенных в прикладное ПО ИПИ-технологий механизмов, которые бы обеспечили управление потоками информации разного уровня конфиденциальности и при этом сняли бы указанные выше ограничения, была проведена НИР. По ее результатам оптимальным вариантом реализации авторами был признан подход с контекстной моделью назначения категорий конфиденциальности. Сеанс конфиденциальности, задаваемый наложенными СрЗИ, в этой модели соответствует максимальному уровню допуска пользователя к информации, но не определяет однозначным образом возможность чтения или записи информации с равной или более низкой категорией конфиденциальности. Вместо этого дополнительно вводится понятие контекста конфиденциальности, который задает текущую категорию конфиденциальности субъекта доступа в пределах контролируемого диспетчером доступа набора операций прикладного ПО (PDM, CAD).

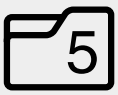
Реализация данного подхода требует весьма существенной переработки основных программных средств ИПИ, как минимум PDM- и CAD-систем, как максимум — всех программных инструментов, позволяющих оперировать информацией с разными категориями конфиденциальности в пределах одного сеанса работы (одного документа). А в связи с особой трактовкой модели Белла-Лападулы могут потребоваться и изменения в нормативных требованиях и руководящих документах по сертификации средств защиты.

В опросе, QR-код с ссылкой на который приведен в конце статьи, сформулированы несколько вопросов к уважаемой аудитории по данной тематике относительно востребованности управления потоками информации в программных средствах ИПИ. Перейдя по ссылке, вы также сможете задать вопросы авторам статьи, на которые они с удовольствием ответят.



Кейс четвертый — об изменениях в организационной структуре

При проектировании процессов в АС было установлено, что из-за возрастающего объема операций передачи информации между базами данных PDM отдельных подразделений (территориально удаленных и организационно самостоятельных) целесообразно выделить отдельный вид администраторов информационной безопасности, отвечающих именно за выполнение и контроль процедур обмена данными (прием заявок на выгрузку обменных пакетов, запись пакетов на носители или файлообменные ресурсы, входной контроль пакетов на целостность, загрузка пакетов).



Кейс пятый — о важности испытаний

На этапе приемочных испытаний было установлено, что инженерное ПО, включая PDM, CAPP, а так же классификаторы НСИ после развертывания СрЗИ НСД стали работать некорректно. Причина была в том, что для работы ПО требуется доступ на запись к различным служебным файлам. При включенной подсистеме полномочного управления доступом (мандатный принцип контроля) доступ к таким файлам осуществляется только в сеансе, мандатная метка которого совпадает с меткой файла, которую он получил при инсталляции. Таким образом, в других сеансах ПО не работает из-за отказа в доступе к служебным файлам ПО. Для устранения проблемы необходимо выполнить ряд настроек в подсистеме полномочного управления доступом СрЗИ НСД.

хитектурой 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 АС, 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 АС со всеми обязательными для такого подхода стадиями. В частности:

1. Должна быть выделена междисциплинарная команда проекта (специалисты по ИТ и ИБ, эксперты по предметным областям автоматизации), которая будет проектировать и вводить в действие АС. Команда должна пройти вводные курсы обучения по всем выбранным для внедрения покупным компонентам (ПО, элементы инфраструктуры), чтобы понимать границы возможностей их адаптации к специфике условий применения. (*См. Кейс № 2)*
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 инфобезопасности.
3. Необходим полноценный этап проектирования АС (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 стороны выполнение требований по защите информации). Одним из актуальных аспектов технологии обработки информации является вопрос управления потоками информации с различным уровнем конфиденциальности *(об этом — Кейс № 3)*;
   В) архитектура АС 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 АС (т.е. их существенную реорганизацию) для того, чтобы меры по защите информации были эффективными, а не формальными. Может потребоваться ввести новые роли в АС 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. (*См. Кейс № 4)*
5. Сдаче АС 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. (*См. Кейс № 5)*

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

Обратная связь

Всем, кто все-таки смог дочитать этот обширный материал до конца, мы предлагаем в режиме онлайн ответить на несколько вопросов и поделиться личным мнением по некоторым важным аспектам рассмотренной темы. Это поможет нам понять, насколько репрезентативен наш опыт в части инфобезопасности в PLM-технологиях. Также вы можете задать нам свои вопросы, на которые мы обязательно постараемся ответить.

Для участия в онлайн-опросе воспользуйтесь QR-кодом или пройдите по ссылке wizard.sd.ascon.ru/index.php/117451