МЕТОДЫ РАЗРАБОТКИ БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СЛОЖНЫХ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ

Михалевич И.Ф.

Институт проблем управления им. В.А. Трапезникова РАН,
Россия, г. Москва, ул. Профсоюзная д.65
mif-orel@mail.ru

Аннотация: Доклад посвящен проблемам разработки программного обеспечения для объектов цифровой экономики и значимых объектов критической информационной инфраструктуры. Методология разработки ориентирована на совместное удовлетворение требований по обеспечению безопасности и технологической независимости в течение всего жизненного цикла программного обеспечения и созданных на его основе информационно-управляющих систем.

Ключевые слова: безопасность программного обеспечения, критическая информационная инфраструктура, метод доверия, метод разработки, информационно-управляющая система, технологическая независимость программного обеспечения.

Введение

В значительном числе случаев условия нарушения безопасности информационных систем, автоматизированных систем управления, информационно-телекоммуникационных сетей возникают в связи с недостаточным вниманием безопасности используемого в них программного обеспечения (ПО). Не редки случаи, когда функции безопасности начинают встраиваться на конечных этапах разработки при тестировании и исправлении ошибок ПО. Такой метод разработки нельзя признать безопасным, несмотря ни на какие уверения.

В условиях возрастающей сложности информационно-управляющих систем (ИУС), составляющих основу национальных цифровых экономик и критических информационных инфраструктур, неизмеримо растет сложность ПО, равно как и цена нарушения его безопасности. В связи с этим методология разработки ПО должна не только учитывать, но и, в определенной степени, подчиняться требованиям безопасности, быть ориентированной на обеспечение безопасности ПО на всех этапах его жизненного цикла. Это влечет необходимость уточнения (изменения) методов разработки ПО с целью повышения оперативности выявления и устранения возможных нарушений безопасности. Реализация концепции безопасного ПО затрагивает не только его разработку, но и процессы создания и функционирования АИУ, а также влечет изменения в сферах профессиональной подготовки лиц, участвующих в разработке ПО, принятии ПО в эксплуатацию, эксплуатации и техническом сопровождении ПО.

1 Методы разработки безопасного программного обеспечения

Безопасным является ПО, которое было разработано с использованием совокупности мер, направленных на предотвращение появления и устранение его уязвимостей [1]. Под уязвимостью

понимается недостаток ПО, который может быть использован для реализации угроз безопасности информации [2]. Недостатком может быть любая ошибка, допущенная в ходе проектирования или реализации программы, которая в случае ее неисправнения может стать причиной ее уязвимости [1].

Появление уязвимостей ПО может быть связано с недостатками в процессах разработки ПО (уязвимости кода, архитектуры, многофакторные), его внедрения, эксплуатации и сопровождения (уязвимости конфигурации, организационные, многофакторные).

Сведения о уязвимостях могут быть предоставлены производителями и сообществами разработчиков ПО. Они могут распространяться регуляторами в области безопасности. Так, например, сведения о уязвимостях ПО аккумулированы в банке данных угроз безопасности информации ФСТЭК России [3], где их поиск может осуществляться как по основным или дополнительным признакам.

При разработке методов разработки и обеспечения безопасности ПО следует учитывать национальные цели и приоритеты, подчиненные им меры по реализации внутренней и внешней национальной политики в сфере применения информационных и коммуникационных технологий. Так, например, в настоящее время реализация внутренней и внешней политики РФ в сфере применения информационных и коммуникационных технологий направлена на развитие информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов [4].

Изменения национальных целей и приоритетов неизбежно влечет изменение критериев безопасности ПО, изменение или уточнение методов его разработки и использования. Об этом свидетельствуют, например, [4], Указ Президента США от 11.05.2017 г. «Об усилении кибербезопасности федеральных сетей и критической инфраструктуры», другие многочисленные нормативные акты РФ, США, ЕС, Китая, других стран и союзов.

Так, например, принятие [4] повлекло уточнение содержания термина и критериев безопасности ПО в РФ. Безопасным будет признано ПО, сертифицированное на соответствие требованиям к информационной безопасности, устанавливаемым уполномоченными федеральными органами исполнительной власти РФ в области обеспечения безопасности противодействия техническим разведкам и технической защиты информации.

Более того, требование безопасности ПО рассматривается совместно с требованием технологической независимости. Согласно [4] технологически независимым является ПО, которое может быть использовано на всей территории РФ, обеспечено гарантийной и технической поддержкой российских организаций, не имеет принудительного обновления и управления из-за рубежа, модернизация которых осуществляется российскими организациями на территории РФ и которые не осуществляют несанкционированную передачу информации, в том числе технологической.

Оба названных требования применяются совместно и совокупно образуют вектор критериев безопасности ПО сложных ИУС. Их несоблюдение исключает возможность признания ПО безопасным, его применение в составе сложных ИУС, таких, например, как значимые объекты критической информационной инфраструктуры, запрещено.

Сложные ИУС подвержены риску нарушения безопасности вследствие многих факторов, возникающих в течение всего жизненного цикла, когда «старение» ИУС проходит на фоне роста типов и видов атак. Увеличение числа потенциальных уязвимостей, сбоев и нарушений обеспечения безопасности ИУС может быть вызвано, в том числе, недооценкой угроз, неудовлетворительной организацией процессов разработки, модернизации и установки обновлений ПО.

В таких условиях владельцы ИУС должны быть не просто уверенными, а определенным образом доверять тому, что использование или развертывание ПО является безопасным, функционирование ПО создает надежные результаты, а меры и средства контроля и управления безопасностью ПО установлены и функционируют должным образом в изменяющихся условиях функционирования ИУС.

Следует учесть, что в контексте безопасности ПО термины «доверие» и «уверенность» не являются идентичными. Следуя подходу, изложенному в [5], примем, что уверенность отражает убежденность в безопасности ПО и является предметом восприятия отдельным лицом специфических требований безопасности и информации, полученной в результате оценки, о том, что ПО удовлетворяет установленным требования.

В отличие от уверенности доверие должно быть основано на доказанной способности ПО обеспечивать выполнение цели безопасности. Основания для утверждения доверия ПО должны базироваться на результатах действий, связанных с проектированием и оценкой безопасности.

Основания доверия должны быть оформлены сертификатом или иным надлежащим национальным документом, отражающим результаты оценки безопасности ПО. Такое свидетельство должно включать в себя аргумент доверия, документацию и другие соответствующие рабочие материалы, подтверждающие результаты оценки.

Угрозы, уязвимости и риски безопасности не статичны. Это требует управления ими в течение жизненного цикла ПО, иначе доверие к ПО может быть утрачено. В связи с этим методы разработки ПО необходимо интегрировать с методами менеджмента рисков безопасности и выявления уязвимостей и угроз, что обеспечит сохранение заданного уровня доверия к безопасности ПО, уверенность в том, что ПО реализует и не нарушает принятую политику безопасности.

Приемлемое доверие означает удовлетворение специальных заранее установленных требований путем выполнения соответствующих процедур и действий по обеспечению доверия в рамках выбранного метода его обеспечения. Совокупные требования доверия определяются исходя из требований безопасности и других факторов [5].

При разработке требований доверия необходимо учитывать факторы возможного влияния на безопасность, возникающие в связи с интересом к сфере применения ПО. Методология разработки безопасного ПО предполагает также проведение анализа конфиденциальности активов, уязвимостей и угроз ИУС, оценку рисков для реализации и корректировки существующих и предполагаемых мер обеспечения безопасности разработки и применения ПО. Недостижение заданного уровня реализации мер влечет пересмотр требований доверия к безопасности ПО, исходя из назначения ИУС. Требования доверия безопасности ПО могут отличаться для различных ИУС вследствие особенностей их назначения и условий функционирования. Одно и то же ПО, пригодное для одних ИУС, может не соответствовать другим ИУС, поскольку для них может быть необходимым удовлетворение других требований доверия.

До последнего времени требования разработки безопасного ПО чаще всего рассматривались в контексте создания защищенных ИУС специального назначения [6-8]. Сегодня, в условиях IoT, Big Date, кибервойск и иных изменившихся условий функционирования сложных АИУС требования безопасности ПО должны стать обязательными и трактоваться таким же образом, как и требования функциональных возможностей, качества и удобства в эксплуатации. Сами же требования безопасности непременно должны быть согласованы с допустимыми пределами остаточного риска уязвимости ПО, как это предложено, например в [9, 10]. В докладе представлено сравнение сфер действия ПО и безопасности ПО, выделены элементы, требующие защиты.

Вопросы безопасности ПО необходимо рассматривать с первых шагов и на всем протяжении его разработки, как это предусмотрено, например, методом SSA (Software security assurance). Данный метод предполагает встраивание функций безопасности на каждом шаге разработки, их совместное тестирование с основными функциями ПО и устранение совместно возникающих ошибок. В докладе представлены процессы жизненного цикла ПО, для которых должна обеспечиваться защита, предложены этапы жизненного цикла разработки безопасного ПО. Предотвращение появления и устранение уязвимостей ПО должно осуществляться во всех процессах жизненного цикла ПО. В докладе приводится анализ мер по разработке безопасного ПО и его сопровождению.

Заключение

Изменение условий функционирования сложных ИУС требует непрерывного внимания к вопросам обеспечения безопасности ПО. Предложенные методы доверия безопасности ПО и разработки безопасного ПО ориентированы на снижение риска нарушения информационной безопасности ИУС в течение их жизненного цикла за счет своевременного выявления угроз и уязвимостей ПО и реализации мер по их устранению.

Литература

1. ГОСТ Р 56939-2016. Защита информации. Разработка безопасного программного обеспечения. Общие требования. Меры по разработке безопасного программного обеспечения. - М.: Стандартинформ, 2016.
2. ГОСТ Р 56546-2015. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. - М.: Стандартинформ, 2015.
3. База данных уязвимостей. - http://bdu.fstec.ru/vul.
4. Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы (утверждена Указом Президента РФ от 09.05.2017 г. № 203).
5. ISO/IEC TR 15443-1:2012. Information technology - Security techniques - Security assurance framework - Part 1: Introduction and concepts. - ISO/IEC: 2012.
6. Проблемы безопасности программного обеспечения. Под ред. П.Д. Зегжда. - СПб: Издательство СПбГТУ, 1995.

7. *Казарин О.В.* Безопасность программного обеспечения компьютерных систем. - М.: МГУЛ, 2003. - 212 с.
8. *Михалевич И.Ф.* Требования, принципы, практика создания отечественных аппаратно-программных платформ для автоматизированных систем в защищенном исполнении критической информационной инфраструктуры Российской Федерации // Интеллектуальные системы. Теория и приложения. - 2018. Том 22, вып. 4. – с. 11- 30.
9. ГОСТ Р ИСО/МЭК 27034-1-2014. Информационная технология. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия. - М.: Стандартинформ, 2015.
10. *Барабанов А.В., Марков А.С., Цирлов В.Л. 2*8 магических мер разработки безопасного программного обеспечения // Вопросы кибербезопасности. 2015. № 5(13). - С. 2-10.