20. Основные принципы обеспечения безопасности ПО на различных стадиях его жизненного цикла

В качестве объекта обеспечения технологической и эксплуатационной безопасности ПО рассматривается вся совокупность его компонентов в рамках конкретной КС. В качестве доминирующей должна использоваться стратегия сквозного тотального контроля технологического и эксплуатационного этапов жизненного цикла компонентов ПО.

Совокупность мероприятий по обеспечению технологической и эксплуатационной безопасности компонентов ПО должна носить конфиденциальный характер. Необходимо обеспечить постоянный, комплексный и действенный контроль за деятельностью разработчиков и пользователей компонентов.

Кроме общих принципов, обычно необходимо конкретизировать принципы обеспечения безопасности ПО на каждом этапе его жизненного цикла. Далее приводятся один из вариантов разработки таких принципов.

Принципы обеспечения технологической безопасности при обосновании, планировании работ и проектном анализе ПО

Принципы обеспечения безопасности ПО на данном этапе включают принципы:

- Комплексности обеспечения безопасности ПО, предполагающей рассмотрение проблемы безопасности информационно - вычислительных процессов с учетом всех структур КС, возможных каналов утечки информации и несанкционированного доступа к ней, времени и условий их возникновения, комплексного применения организационных и технических мероприятий.
- Планируемости применения средств безопасности программ, предполагающей перенос акцента на совместное системное проектирование ПО и средств его безопасности, планирование их использования в предполагаемых условиях эксплуатации.
- Обоснованности средств обеспечения безопасности ПО, заключающейся в глубоком научно-обоснованном подходе к принятию проектных решений по оценке степени безопасности, прогнозированию угроз безопасности, всесторонней априорной оценке показателей средств защиты.
- Достаточности безопасности программ, отражающей необходимость поиска наиболее эффективных и надежных мер безопасности при одновременной минимизации их стоимости.
- Гибкости управления защитой программ, требующей от системы контроля и управления обеспечением информационной безопасности ПО способности к диагностированию, опережающей нейтрализации, оперативному и эффективному устранению возникающих угроз в условиях резких изменений обстановки информационной борьбы.
- Заблаговременности разработки средств обеспечения безопасности и контроля производства ПО, заключающейся в предупредительном характере мер обеспечения технологической безопасности работ в интересах недопущения снижения эффективности системы безопасности процесса создания ПО.
- Документируемости технологии создания программ, подразумевающей разработку пакета нормативно-технических документов по контролю программных средств на наличие преднамеренных дефектов.

Принципы достижения технологической безопасности ПО в процессе его разработки

Принципы обеспечения безопасности ПО на данном этапе включают принципы:

- Регламентации технологических этапов разработки ПО, включающей упорядоченные фазы промежуточного контроля, спецификацию программных модулей и стандартизацию функций и формата представления данных.
- Автоматизации средств контроля управляющих и вычислительных программ на наличие дефектов, создания типовой общей информационной базы алгоритмов, исходных текстов и программных средств, позволяющих выявлять преднамеренные программные дефекты.

- Последовательной многоуровневой фильтрации программных модулей в процессе их создания с применением функционального дублирования разработок и поэтапного контроля.
- Типизации алгоритмов, программ и средств информационной безопасности, обеспечивающей информационную, технологическую и программную совместимость, на основе максимальной их унификации по всем компонентам и интерфейсам.
- Централизованного управления базами данных проектов ПО и администрирование технологии их разработки с жестким разграничением функций, ограничением доступа в соответствии со средствами диагностики, контроля и защиты.
- Блокирования несанкционированного доступа соисполнителей и абонентов государственных сетей связи, подключенных к стендам для разработки программ.
- Статистического учета и ведения системных журналов о всех процессах разработки ПО с целью контроля технологической безопасности.
- Использования только сертифицированных и выбранных в качестве единых инструментальных средств разработки программ для новых технологий обработки информации и перспективных архитектур вычислительных систем.
- Принципы обеспечения технологической безопасности на этапах стендовых и приемо-сдаточных испытаний

Принципы обеспечения безопасности ПО на данном этапе включают принципы:

- Тестирования ПО на основе разработки комплексов тестов, параметризуемых на конкретные классы программ с возможностью функционального и статистического контроля в широком диапазоне изменения входных и выходных данных.
- Проведения натурных испытаний программ при экстремальных нагрузках с имитацией воздействия активных дефектов.
- Осуществления "фильтрации" программных комплексов с целью выявления возможных преднамеренных дефектов определенного назначения на базе создания моделей угроз и соответствующих сканирующих программных средств.
- Разработки и экспериментальной отработки средств верификации программных изделий.
- Проведения стендовых испытаний ПО для определения непреднамеренных программных ошибок проектирования и ошибок разработчика, приводящих к невыполнению целевых функций программ, а также выявление потенциально "узких" мест в программных средствах для разрушительного воздействия.
- Отработки средств защиты от несанкционированного воздействия нарушителей на ПО.
- Сертификации программных изделий АСУ по требованиям безопасности с выпуском сертификата соответствия этого изделия требованиям технического задания.

Принципы обеспечения безопасности при эксплуатации программного обеспечения

Принципы обеспечения безопасности ПО на данном этапе включают принципы:

- Сохранения и ограничения доступа к эталонам программных средств, недопущение внесения изменений в них.
- Профилактического выборочного тестирования и полного сканирования программных средств на наличие преднамеренных дефектов.
- Идентификации ПО на момент ввода его в эксплуатацию в соответствии с предполагаемыми угрозами безопасности ПО и его контроль.
- Обеспечения модификации программных изделий во время их эксплуатации путем замены отдельных модулей без изменения общей структуры и связей с другими модулями.
- Строгого учета и каталогизации всех сопровождаемых программных средств, а также собираемой, обрабатываемой и хранимой информации.
- Статистического анализа информации обо всех процессах, рабочих операциях, отступлениях от режимов штатного функционирования ПО.
- Гибкого применения дополнительных средств защиты ПО в случае выявления новых, непрогнозируемых угроз информационной безопасности.

Хакерская атака в узком смысле слова — в настоящее время под словосочетанием понимается «Покушение на систему безопасности», и склоняется скорее к смыслу следующего термина Крэкерская атака. Это произошло из-за искажения смысла самого слова «хакер».

Хакерская атака в широком смысле слова (изначальный смысл) — мозговой штурм, направленный на нахождение пути решения сложных задач. В хакерской атаке могут принимать участие один или несколько высококлассных специалистов (хакеров). В результате мозгового штурма могут быть придуманы нетрадиционные методы решения проблемы, или внесены оптимизирующие корректировки в уже существующие методы.

Крэкерская атака — действие, целью которого является захват контроля (повышение прав) над удалённой/локальной вычислительной системой, либо её дестабилизация, либо отказ в обслуживании.

Считается самым старым методом атак, хотя суть его проста и примитивна: большое количество почтовых сообщений делают невозможными работу с почтовыми ящиками, а иногда и с целыми почтовыми серверами. Для этой цели было разработано множество программ, и даже неопытный пользователь мог совершить атаку, указав всего лишь e-mail жертвы, текст сообщения, и количество необходимых сообщений.

Многие такие программы позволяли прятать реальный IP-адресов отправителя, используя для рассылки анонимный почтовый сервер. Эту атаку сложно предотвратить, так как даже почтовые фильтры провайдеров не могут определить реального отправителя спама. Провайдер может ограничить количество писем от одного отправителя, но адрес отправителя и тема зачастую генерируются случайным образом.

Переполнение буфера

Пожалуй, один из самых распространенных типов атак в Интернете. Принцип данной атаки построен на использовании программных ошибок, позволяющих вызвать нарушение границ памяти и аварийно завершить приложение или выполнить произвольный бинарный код от имени пользователя, под которым работала уязвимая программа.

Если программа работает под учётной записью администратора системы, то данная атака позволит получить полный контроль над компьютером жертвы, поэтому рекомендуется работать под учётной записью рядового пользователя, имеющего ограниченные права на системе, а под учётной записью администратора системы выполнять только операции, требующие административные права.