«Выявление и устранение уязвимостей в информационных системах»

Заместитель начальника отдела
Носов Игорь Анатольевич

Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах

…выявление и устранение уязвимостей в информационных системах;

…выявление и реагирование на инциденты безопасности информации в информационных системах

Задачами выявления инцидентов безопасности и реагирования на них являются:

обнаружение, оповещение об инцидентах безопасности и их оценка;

реагирование на инциденты безопасности, включая активацию соответствующих мер защиты для предотвращения, уменьшения последствий и (или) восстановления системы после негативных воздействий;

анализ причин возникновения инцидента безопасности;

введение превентивных мер защиты и совершенствования системы защиты

Документы национальной системы стандартизации

Национальный стандарт ГОСТ Р ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»;

Национальный стандарт ГОСТ Р 54141-2010 «Менеджмент рисков. Руководство по применению организационных мер безопасности и оценки рисков. Эталонные сценарии инцидентов»;

Национальный стандарт ГОСТ Р 54142-2010 «Менеджмент рисков. Руководство по применению организационных мер безопасности и оценки рисков. Методология построения универсального дерева событий»;

Национальный стандарт ГОСТ Р 54144-2010 «Менеджмент рисков. Руководство по применению организационных мер безопасности и оценки рисков. Идентификация инцидентов»

Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах

пп. 14.3: *«Угрозы безопасности информации определяются по результатам оценки возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей, анализа возможных уязвимостей информационной системы, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).*

Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах

пп. 15.1 *«При проектировании системы защиты информации информационной системы:*

…

определяются параметры настройки программного обеспечения, включая программное обеспечение средств защиты информации, обеспечивающие реализацию мер защиты информации, ***а также устранение возможных уязвимостей информационной системы, приводящих к возникновению угроз безопасности информации;***

определяются меры защиты информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, в том числе с информационными системами уполномоченного лица, а также при применении вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации».

Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах

п. 16: *«Внедрение системы защиты информации информационной системы организуется обладателем информации (заказчиком).*

Внедрение системы защиты информации информационной системы осуществляется в соответствии с проектной и эксплуатационной документацией на систему защиты информации информационной системы и в том числе включает:

…

анализ уязвимостей информационной системы и принятие мер защиты информации по их устранению».

Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах

пп. 16.6 *«Анализ уязвимостей информационной системы проводится в целях оценки возможности преодоления нарушителем системы защиты информации информационной системы и предотвращения реализации угроз безопасности информации.*
Анализ уязвимостей информационной системы включает анализ уязвимостей средств защиты информации, технических средств и программного обеспечения информационной системы.
При анализе уязвимостей информационной системы проверяется отсутствие известных уязвимостей средств защиты информации, технических средств и программного обеспечения, в том числе с учетом информации, имеющейся у разработчиков и полученной из других общедоступных источников, правильность установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректность работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением…

Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах

пп. 17.1: *«В качестве исходных данных, необходимых для аттестации информационной системы, используются модель угроз безопасности информации, акт классификации информационной системы, техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание системы защиты информации информационной системы, проектная и эксплуатационная документация на систему защиты информации информационной системы, организационно-распорядительные документы по защите информации, результаты анализа уязвимостей информационной системы, материалы предварительных и приемочных испытаний системы защиты информации информационной системы, а также иные документы, разрабатываемые в соответствии с настоящими Требованиями».*

информации, проводится уточнение модели угроз безопасности информации и при необходимости принимаются дополнительные меры защиты информации, направленные на устранение выявленных уязвимостей или исключающие возможность использования нарушителем выявленных уязвимостей».

приложение № 2 к Требованиям
группа мер Контроль (анализ) защищенности информации

АН3.1 «Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей»;
АН3.2 «Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации»;
АН3.3 «Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации»;
АН3.4 ««Контроль состава технических средств, программного обеспечения и средств защиты информации»;
АН3.5 ««Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе».

методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утверждённый 11 февраля 2014г.

ОПС.2 *«Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения»*

«Требования к реализации ОПС.2: *Оператором должны быть реализованы следующие функции по управлению установкой (инсталляцией) компонентов программного обеспечения информационной системы:*

…

определение и применение параметров настройки компонентов программного обеспечения, включая программные компоненты средств защиты информации, обеспечивающих реализацию мер защиты информации, а также устранение возможных уязвимостей информационной системы, приводящих к возникновению угроз безопасности информации».

Меры защиты информации в государственных информационных системах

(РСБ.5) *«Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них» (мера обязательная)*

«Требования к усилению РСБ.5:

…

2)в информационной системе обеспечивается ***интеграция процессов мониторинга*** *(просмотра, анализа) результатов регистрации событий безопасности* ***с результатами анализа уязвимостей****, проводимого в соответствии с АНЗ.1, и результатами обнаружения вторжений, проводимого в соответствии с СОВ.1 с целью усиления возможностей по выявлению признаков инцидентов безопасности (усиление не обязательное)».*

Меры защиты информации в государственных информационных системах

АНЗ.1 *«Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей» (мера обязательная для 1, 2 и 3 классов защищенности ИС)*

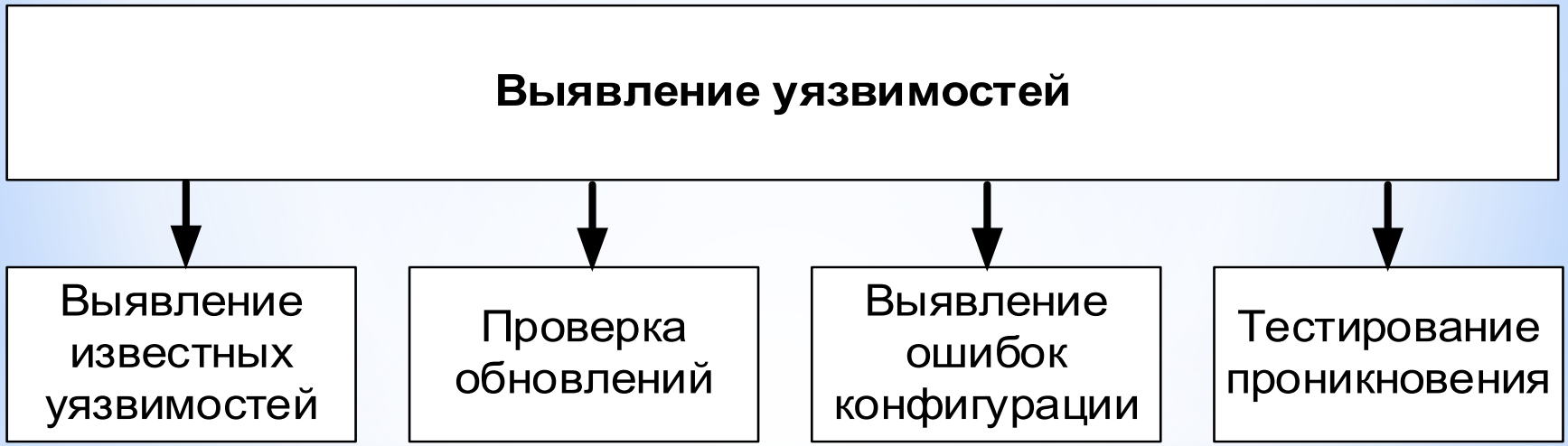
При выявлении (поиске), анализе и устранении уязвимостей в информационной системе должны проводиться:
выявление (поиск) уязвимостей…
разработка по результатам выявления (поиска) уязвимостей отчетов …
анализ отчетов с результатами поиска уязвимостей …
устранение выявленных уязвимостей…
информирование должностных лиц…

Меры защиты информации в государственных информационных системах

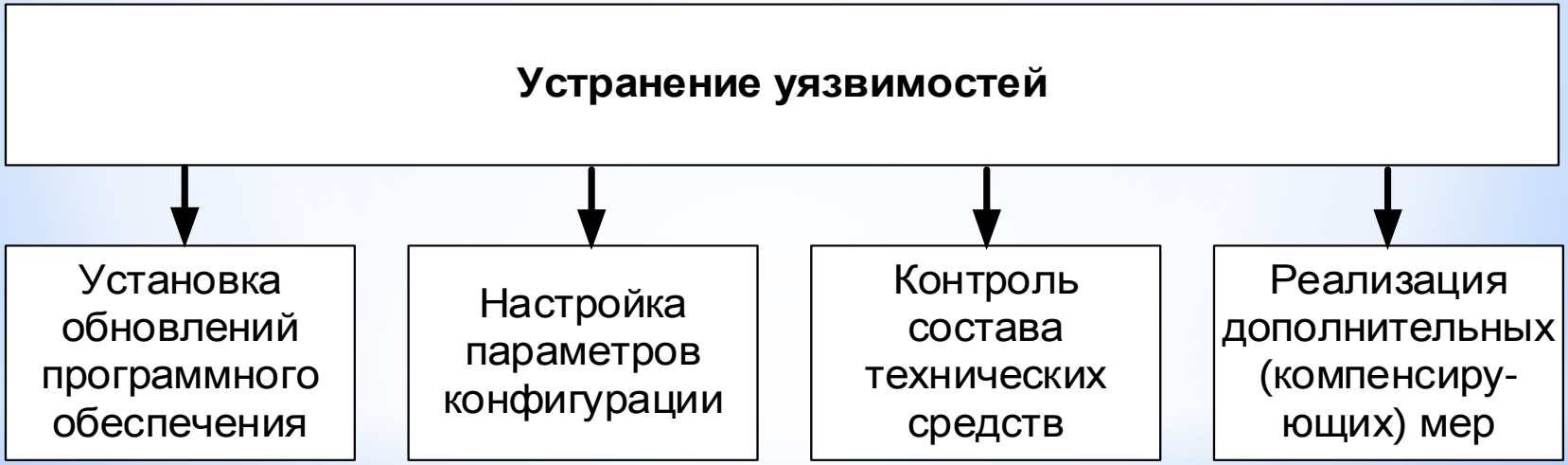
ЗИС.25 «Использование в информационной системе или ее сегментах различных типов общесистемного, прикладного и специального программного обеспечения (создание гетерогенной среды)» (мера не обязательная)

Требования к реализации ЗИС.25:
При создании гетерогенной среды необходимо учитывать повышение сложности в управлении конфигурацией информационной системы и возможность увеличения ошибок конфигурации и возможных уязвимостей».

Проведение работ по выявлению уязвимостей



Проведение работ по устранению уязвимостей



Процесс выявления и устранения уязвимостей программно-аппаратных средств обработки информации в информационной системе

Постановление Правительства РФ от 15.06.2016 N 541 «О внесении изменений в некоторые акты Правительства Российской Федерации по вопросам лицензирования отдельных видов деятельности»

4. При осуществлении деятельности по технической защите конфиденциальной информации лицензированию подлежат следующие виды работ и услуг:

б) контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;

лицензируемыми видами деятельности являются мониторинг информационной безопасности, контроль защищенности...

«Выявление и устранение уязвимостей в информационных системах»

Заместитель начальника отдела
Носов Игорь Анатольевич