# ИНФОРМАЦИОННОЕ СООБЩЕНИЕ
## о повышении безопасности средств защиты информации, в состав которых разработчики включают интерпретаторы (компоненты среды функционирования интерпретируемых языков или языков, компилируемых в промежуточное представление), веб-сервера и сервера приложений или задействуют для реализации функциональных возможностей средств данные программные компоненты из состава среды функционирования

Изготовители средств защиты информации от несанкционированного доступа (далее — средства защиты информации) включают в состав средств защиты информации интерпретаторы (компоненты среды функционирования интерпретируемых языков или языков, компилируемых в промежуточное представление), веб-сервера и сервера приложений или задействуют для реализации функциональных возможностей средств защиты информации данные программные компоненты из состава среды функционирования.

Применение таких программных компонентов влияет на эффективность применения и безопасность средств защиты информации в связи с наличием в них функций безопасности, используемых средством защиты информации, избыточных полномочий и уязвимостей.

В целях повышения безопасности средств защиты информации, использующих указанные программные компоненты, при разработке и сертификации необходимо:

1. В случае использования средством защиты информации для реализации функций безопасности или в составе поверхности атаки средства защиты информации интерпретаторов, веб-серверов и серверов приложений из состава среды функционирования средства защиты информации, они должны быть сертифицированы по требованиям безопасности информации.

Интерпретаторы, веб-сервера и сервера приложений могут быть сертифицированы самостоятельно, в составе среды функционирования средства защиты информации, или в составе средства защиты информации.

2. В случае включения в состав операционных систем несертифицированных интерпретаторов, веб-серверов и серверов приложений ко всем функциям по безопасности, содержащихся в указанных компонентах, предъявляются требования по безопасности информации, которые должны быть включены в технические условия на операционную систему и выполнение которых проверяется при проведении сертификационных испытаний. Кроме того, данные компоненты должны пройти испытания по выявлению уязвимостей и недекларированных возможностей в соответствии с Методикой выявления уязвимостей и недекларированных возможностей в программном обеспечении, утвержденной ФСТЭК России 25 декабря 2020 г., в полном объеме.

3. В случае включения в состав иных средств защиты информации несертифицированных интерпретаторов, веб-серверов и серверов приложений данные компоненты проходят сертификационные испытания в составе средств защиты информации в части задействования данных компонентов при реализации функций безопасности средств защиты информации или в поверхности атаки средств защиты информации.

4. В средстве защиты информации должна быть минимизирована поверхность атаки за счет исключения неиспользуемых кода и функциональных возможностей на этапе сборки средства защиты информации.

5. Компоненты, используемые в средстве защиты информации или задействованные средством защиты информации из среды его функционирования, в том числе интерпретаторы, веб-сервера и сервера приложений, должны наделяться полномочиями, минимально необходимыми для функционирования средства защиты информации. Избыточные полномочия компонентов, выявленные при проведении сертификации средства защиты информации, должны быть устранены.

6. Веб-сервера и сервера приложений из состава средства защиты информации или используемые средством защиты информации, включающие в себя функциональные возможности по выполнению кода, должны допускать выполнение кода либо входящего в состав средства защиты информации, либо допущенного к выполнению посредством документированных функциональных возможностей средства защиты информации, обеспечивая при этом целостность кода при его хранении.

7. В эксплуатационную документацию средств защиты информации, в том числе интерпретаторов, веб-серверов и серверов приложений, должны быть

включены сведения о всех функциональных возможностях, в том числе функциях безопасности, параметрах их безопасной конфигурации, настройки и эксплуатации, а также рекомендации по контролю безопасной конфигурации и настройки средств.

Первый заместитель директора В.Лютиков