# Валерий Ледовской (Spacebit):

# Запрос на ИБ идет именно от рынка

**Проблема безопасности настроек ПО известна достаточно давно и входит в состав любой ИБ-концепции. Но есть тонкости и нюансы. О них «Б.О» рассказал Валерий Ледовской, BDM по продукту X-Config компании Spacebit**



*Текст*
**ВАДИМ ФЕРЕНЕЦ,**
ОБОЗРЕВАТЕЛЬ **«Б.О»**

**— Валерий, что представляет собой рынок управления безопасностью конфигурирования ПО?**
— Этот рынок является неотъемлемой частью области управления уязвимостями, которая становится весьма актуальной: от 50% фактов утечек данных так или иначе связаны с небезопасными настройками ПО либо оборудования.

В целом, управление уязвимостями можно условно разбить на несколько составляющих относительно жизненного цикла программного продукта. Во-первых, это уязвимости архитектуры ПО, то есть на уровне функциональных связей компонентов ПО. Во-вторых, уязвимости реализации — это уязвимости на уровне программного кода. И, наконец, уязвимости при эксплуатации ПО — это уязвимости в сценариях использования программ и корректности применяемых настроек. И если вопрос устранения уязвимостей на архитектурном уровне и на уровне программного кода — задача вендора, то за безопасностью использования ПО необходимо следить самим организациям, которые его эксплуатируют.

К сожалению, во многих организациях так и не был выстроен эффективный автоматический процесс безопасной настройки используемого ПО. Чаще всего он проводится вручную с привлечением собственной экспертизы и эпизодическим, нерегулярным аудитом безопасности конфигурации. Эти процессы редко бывают эффективными и не позволяют контролировать настройки используемого ПО в постоянном режиме.

В целом же, в мире, в частности в России, проблема безопасности настроек ПО стоит давно. Требования по этой теме есть как у зарубежных, так и у российских регуляторов, а также прописаны в лучших международных практиках, касающихся разработок стандартов безопасного конфигурирования для популярного ПО, но при этом на практике соответствующие процессы не работают.

**— Существует ли конкуренция на рынке?**
— Она, безусловно, есть, и ее усиление в последнее время подчеркивает важность организации эффективного контроля





безопасности конфигураций. При этом мы считаем основным стимулом развития не требования регуляторов, а необходимость обеспечения кибербезопасности инфраструктур из-за значительного увеличения количества успешных кибератак. Этот запрос идет непосредственно от рынка.

К непрямым конкурентам X-Config от компании Spacebit мы относим, например, сканеры уязвимостей, которые сканируют в том числе и конфигурацию ПО с точки зрения безопасности настроек, но эти инструменты больше предназначены для проведения периодических аудитов ИБ.

К прямым конкурентам можно отнести несколько российских продуктов, близких к нам по функциональности, в этих системах реализованы разные степени свободы с точки зрения гибкости инструментов. Но X-Config при этом может легко масштабироваться, что позволяет использовать его во многих конфигурациях — от небольших сетей до гигантских инфраструктур. А реализованное профилирование стандартов безопасного конфигурирования дает возможность учесть особенности любой инфраструктуры и бизнес-процессов.

**— Требования каких нормативных актов закрываются решением?**
— Что касается финансовой сферы, то здесь можно выделить несколько основных регуляторов. Во-первых, это стандарт PCI DSS, неизменно актуальный в нашей стране и по сей день, несмотря на все санкции. Во-вторых, финансовые организации являются субъектами критической информационной инфраструктуры (КИИ), а значит, регулируются со стороны ФСТЭК и ФСБ соответствующими федеральными законами и приказами этих ведомств. Наконец, не стоит забывать и о требованиях отраслевого регулятора, Банка России, содержащихся в основном стандарте — ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций». Соответствующие требования этих нормативных актов можно закрыть с помощью решения X-Config.

**— Можно ли утверждать, что X-Config позволяет сократить риск человеческого фактора? За счет чего?**
— Можно сказать, что X-Config посвящен именно снижению риска человеческого фактора. С одной стороны, минимизируются риски ошибочных или сознательных действий пользователей и администраторов, которые не приводят настройки используемого ПО в безопасное состояние. С другой стороны, мы резко снижаем потребность в наличии сотрудников с серьезной экспертизой в области безопасной настройки всего используемого стека технологий. Она остается лишь на этапе построения профилей безопасного конфигурирования, и то в очень ограниченном объеме.

**— Используются ли стандарты безопасного конфигурирования?**
— Да, мы используем лучшие мировые практики, оформленные в виде соответствующих бенчмарков со списком требований к конфигурациям ПО в тех случаях, когда они применимы. Но в любом случае эти требования проходят ревизию наших аудиторов и дополняются требованиями регуляторов.

В последнее время в X-Config появляется поддержка все большего объема российского системного и прикладного ПО, для которого нет в открытом доступе бенчмарков. Поэтому мы создаем технологические партнерства с ведущими отечественными IT-вендорами, получаем необходимую информацию от них. Кроме того, в составе продукта мы предлагаем для каждого стандарта безопасного конфигурирования профили, полностью соответствующие требованиям регуляторов, под действие которых попадают наши заказчики.

В X-Config реализована возможность утверждения профилей безопасного конфигурирования как части ИБ-политики предприятия. Кроме того, реализовано разделение ролей офицеров ИБ и системных администраторов.

**— Какова архитектура X-Config и из каких компонентов состоит решение?**
— Архитектура X-Config состоит из нескольких основных компонентов: ядра системы, клиентской части и сети управляемых коллекторов. Ядро собирает информацию о конфигурациях ПО с защищаемых хостов, а также анализирует ее для выявления несоответствий. Клиентская часть выполнена в виде веб-приложения, в графическом интерфейсе которого реализованы все необходимые сценарии использования решения.

Управляемые коллекторы собирают с защищаемых машин информацию о конфигурации ПО и передают ее на ядро системы. Из коллекторов строится сеть, которая позволяет масштабировать систему из 10 тыс. хостов и более. Кроме того, система позволяет распределять группы коллекторов между различными подсетями, поддерживая идеологию сегментирования крупных сетей.

X-Config может выступать полноценной частью экосистемы кибербезопасности организаций и экономить ресурсы на свое обслуживание. В частности, вместо использования встроенного механизма инвентаризации информацию о контролируемых ресурсах сети можно передавать в X-Config через интеграцию с уже работающей CMDB, а результаты проверок безопасности настроек можно передавать в системы SIEM, SOAR, IRP и другие через встроенный API.

X-Config поставляется в двух вариантах: Business-редакция и Enterprise-редакция. Первая предназначена для небольших инфраструктур (до 500 хостов), вторая — для более крупных инфраструктур. В итоговую сумму входят лицензия на необходимое количество защищаемых хостов, а также базовая техническая поддержка, которая осуществляется силами вендора. Кроме того, мы можем поддержать за отдельную плату необходимые дополнительные функции, а также разработать новые стандарты безопасного конфигурирования для специального отраслевого ПО, включая самописное.

Добавлю в финале, что все продукты компании Spacebit, включая X-Control, объединяет автоматизация рутинных процессов ИБ, что позволяет высвободить рабочее время специалистов для решения более приоритетных задач, связанных с повышением уровня безопасности инфраструктур. **Б.О**