Кибериммунность ИТ-инфраструктуры
на уровне операционной системы

Игорь КОРЧАГИН,
руководитель департамента информационной безопасности, АО ИВК

Россия взяла курс на технологический суверенитет, и в ИТ-инфраструктуре заказчиков появился новый пласт решений – операционные системы на ядре Linux. Как следствие, сместился привычный вектор атак, а вместе с этим изменился подход к решению вопросов безопасности, в том числе в части разработки операционных систем.

Почти все деловые процессы госсектора и бизнеса переведены на цифру, поэтому цифровая инфраструктура – привлекательный объект для злоумышленников. Число и изощренность кибератак стремительно растут. Так, в первой половине 2023 г. количество инцидентов в области кибербезопасности на четверть превысило показатели предыдущего полугодия. Например, согласно отчету компании «РТК-Солар», только во втором квартале текущего года было выявлено 325 тыс. инцидентов в области информационной безопасности, что на 12% больше, чем в первом квартале, и на 38% превышает показатель аналогичного периода прошлого года.

Рост числа атак на российские организации и предприятия во многом обусловлен обострением геополитической обстановки. Ситуация усугубляется активным уходом с рынка зарубежных вендоров, прекращением поддержки ранее поставленных программных продуктов, блокировкой лицензий на используемое ПО.

Тенденция к увеличению количества и усилению интенсивности кибератак на объекты КИИ опасна для отраслей и сегментов российской экономики. А для некоторых предприятий и организаций она может оказаться фатальной. Поэтому инфраструктуру, прежде всего критическую информационную, надо как можно быстрее перевести на защищенное сертифицированное российское программное обеспечение и оборудование. И в первую очередь – на российские операционные системы.

На базе независимой инфраструктуры разработки

Гарантией защиты ИТ-инфраструктуры от многих деструктивных воздействий служит разработка операционной системы на основе инфраструктуры, находящейся на территории и под юрисдикцией Российской Федерации. Ключевым элементом такой инфраструктуры служит репозиторий – хранилище программных пакетов, из которых собирается операционная система.

Если российские разработчики полностью контролируют свою инфраструктуру разработки, вероятность появления уязвимостей в коде операционной системы существенно снижается. Собственные технологии позволяют организовать воспроизводимую сборку и значительно снизить вероятность проведения успешных атак на пакетную базу, сборочную инфраструктуру и готовые программные продукты. Можно привести в пример семейство операционных систем, жизненный цикл которых реализуется на основе российского репозитория проекта Sisyphus (Сизиф) – одного из крупнейших в мире технологически независимых репозиториев наряду с Debian, Red Hat и SUSE. Для разработки таких ОС применяется система сборки пакетов в изолированном окружении, позволяющая исключить влияние не только сборочного узла на собираемый пакет, но и процесса сборки на сборочный узел.

Инфраструктура разработки защищенных российских ОС строится с учетом требований международных и российских стандартов и нормативных документов, в частности ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования». Эти документы обобщают лучший современный мировой опыт

разработки программных продуктов на всех стадиях жизненного цикла – от проектирования и разработки новых версий до серийного производства и технической поддержки внедренных у заказчика решений.

На основе указанных требований строится система качества компании-разработчика, четко описывающая комплекс технологических операций и организационных мер, которые реализуются при разработке и серийном производстве программных продуктов. Система регламентирует производственные процессы, обязанности и ответственность персонала (от рядовых сотрудников до высшего руководства), ведение проектно-конструкторской, технологической, эксплуатационной и нормативно-технической документации, организацию послепродажного обслуживания и т. п.

В ходе разработки программные продукты тщательно исследуются на предмет выявления ошибок и уязвимостей средствами статического и динамического анализа, в том числе фаззинг-тестирования.

Сотрудничество как фактор повышения защищенности ОС

Уровень защищенности ОС повышает сотрудничество с международными проектами СПО. Развитие ОС на основе ядра Linux неразрывно связано с изменениями кода, в том числе в части кибербезопасности. Реализовать эти изменения в одиночку не способна ни одна компания-разработчик в мире. Распределять нагрузку позволяет международная кооперация разработчиков свободного ПО. Проекты обмениваются своими наработками, из которых затем собираются готовые программные продукты. Способ разработки всем миром ускоряет и удешевляет процессы создания ПО.

Кооперация с международными проектами дает возможность вести поиск уязвимостей в коде сообща, что повышает защищенность продукта. Так, формальное закрытие уязвимостей, известных на российском рынке ОС, происходит одновременно с основными международными дистрибутивами, а фактическое – до обнародования информации о найденной уязвимости в публичных банках данных об уязвимостях. Разработчики этих ОС входят в число международных сообществ экспертов, принимающих решения о дате публикации сообщений о выявленных уязвимостях.

Кроме того, если российские программисты участвуют в международных проектах разработки СПО, их программные продукты развиваются в ногу с мировыми тенденциями. Например, российские специалисты – участники таких ключевых международных проектов, как kernel (проект, который разрабатывает ядро Linux), glibc (библиотека Си, которая обеспечивает системные вызовы и основные функции ПО) и др.

Следует отметить, что разработчики российских ОС должны передавать свои наработки в международные проекты, чтобы они дальше развивались с учетом изменений, внесенных отечественными разработчиками. Это важно по двум причинам. Во-первых, международным разработкам придаются свойства, важные для российских пользователей. Например, криптографические библиотеки, поддерживающие стандарты шифрования российских ГОСТов. Во-вторых, чтобы объем изменений не стал неконтролируемым. Если разработчики базовых проектов не учтут произошедшие в российской ОС изменения, то с каждой новой версией ОС трудоемкость применения изменений будет повышаться и со временем задача станет невыполнимой.

Так, например, разработчики ОС «Альт» участвуют в международных проектах – их код есть в ядре Linux (в том числе и реализация российского крипто с поддержкой стандартов шифрования семейства ГОСТ), в основных системных библиотеках и других ключевых компонентах свободного ПО, в свободных средствах защиты информации, средствах удаленного доступа и т. д.

Опережающее устранение уязвимостей

Обнаружение уязвимостей должно быть заложено в модель разработки операционной системы. Именно такую модель построили ведущие российские компании для разработки семейства операционных систем, в том числе защищенной ОС для серверов и рабочих станций. На разных стадиях разработки эксперты составляют индивидуальную карту поверхности атак, отмечают на ней потенциально опасные области.

Затем каждая из областей всесторонне исследуется с помощью комплекса различных инструментов статического и динамического анализа программного кода. В ходе исследования используются новейшие методики, созданные российским и международным ИТ-сообществом, а также собственные наработки.

Технологическая пара «процессор – операционная система»

Миграция на российскую ОС – полдела. Для обеспечения полной безопасности ИТ-инфраструктуры организации ее необходимо перевести на оборудование, включенное в Единый реестр радиоэлектронной продукции Минпромторга, в первую очередь на компьютеры с процессорами «Эльбрус». Они развиваются на архитектуре, которая разработана российскими инженерами, интеллектуальная собственность принадлежит России. По своим потребительским свойствам компьютеры «Эльбрус» не уступают компьютерам с процессорами Intel и AMD. Это регулярно отмечают ИТ-специалисты и сотрудники организаций, которые используют серверы и рабочие станции «Эльбрус».

Операционная система должна взаимодействовать с процессором «Эльбрус» в нативных кодах, т. е.

без необходимости имитировать работу процессора Intel, что позволяет использовать максимальную производительность российского процессора.

Особое внимание безопасности ядра Linux

Сегодня российское ИТ-сообщество консолидируется, чтобы сообща обнаруживать уязвимости в свободном ПО. Под эгидой Института системного программирования им. В.П. Иванникова Российской Академии наук (ИСП РАН) сформировалось сообщество по безопасной разработке. На базе ИСП РАН под эгидой ФСТЭК России создан Центр исследования безопасности ядра Linux. Цель – в рамках реализации федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации» повысить уровень безопасности отечественных систем на базе ядра Linux.

Для повышения эффективности взаимодействия в рамках Технологического центра разработчики объединились в Консорциум участников по поддержке Технологического центра. В круг интересов консорциума входят внедрение принципов безопасной разработки программного обеспечения и исключение дублирования усилий по исследованию безопасности ядра Linux. Совместные усилия российских разработчиков повысят кибериммунность операционных систем, ключевого компонента цифровой инфраструктуры миллионов российских организаций и предприятий, которые работают в государственном и коммерческом секторах российской экономики. ■

Совместимость для реестра

Отечественных разработчиков ПО попросят адаптировать его под работу с российскими операционными системами. Правила включения софта в реестр отечественного ПО могут стать жестче – речь идет о совместимости минимум с двумя российскими операционными системами. Для преференций на госзакупках продукт должен быть совместим также хотя бы с одним процессором из реестра Минпромторга.

Минцифры планирует внести поправки в постановления, которые регулируют процедуру включения российского софта в реестр отечественного программного обеспечения, сообщает «Коммерсант». Согласно документу, на который ссылаются СМИ, министерство планирует ввести требование для разработчиков ПО адаптировать софт, который планируют внести в реестр, под работу как минимум с двумя российскими операционными системами. Для того чтобы разработчик софта также получил преференции на закупках, ПО должно быть совместимо и с российскими процессорами из реестра Минпромторга.

По данным источников СМИ, документ уже направлен на обсуждение в профильные компании. В Минцифры сообщили изданию, что рассчитывают утвердить новые правила уже в этом году, но вступать в силу они будут «поэтапно начиная с 2024 года». «Совместимость с отечественным процессором не будет обязательной для включения в реестр, но позволит соответствовать дополнительным требованиям, имеющим значение для потенциальных заказчиков», – уточнили в министерстве.

Разработка ПО и его адаптация для работы с ОС – процесс длительный, в связи с чем Минцифры «уже сейчас озаботилось введением таких требований, это в полной мере соответствует стратегии развития микроэлектроники в России», отметили в Минпромторге.

Как сообщили в ассоциации «Руссофт», доля российских компаний, разрабатывающих приложения для Windows, уже снизилась до 68%, в то время как в 2020–2022 гг. показатель находился на уровне 74–79%, а ранее – 94–97%. Доли Android, iOS и Mac OS в общем объеме использования операционных систем по итогам 2022 г. также снизились в полтора-два раза.

Минцифры РФ намерено инициировать создание независимых центров тестирования совместимости отечественного софта с российским оборудованием и операционными системами. Такие центры по заявлению смогут оценивать по единым стандартам совместимость российского софта с российским оборудованием и операционными системами. Ранее сообщалось, что обсуждается проект, вопрос бюджетного финансирования, порядок аккредитации центров и оценка качества работы. При этом сроки создания таких центров пока не определены.