

10. Сообщайте об уязвимостях по правилам Китая: до исправления не раскрывайте детали, не публикуйте инструменты для их использования и не передавайте сведения за рубеж

Выгодность исходной версии: высокая

Доказательность А · исходная версия

для свободы

бесплатно

мимоходом

без силы воли

Частично Китай

Аналог в России не найден

Искали в официальных российских источниках (проверено 08.10.2026), прямого аналога не нашли. Это не значит, что его нет. Китайские условия на Россию не переносите.

Оценки выше относятся к исходной версии; отдельная оценка российского варианта не проводилась.

Простыми словами

Китай — исходная версия. На частных лиц в Китае тоже распространяются «Правила управления уязвимостями безопасности сетевых продуктов (网络安全漏洞管理规定)». Пока производитель не предложит меры по исправлению, вы не можете публиковать сведения об уязвимости. Нельзя также раскрывать детали уязвимостей систем, которые используются в данный момент. Нельзя публиковать программы и инструменты, специально предназначенные для использования уязвимостей. При публикации нужно одновременно объяснить, как исправить уязвимость. Неопубликованные сведения об уязвимостях нельзя передавать организациям и частным лицам за рубежом, кроме производителя.

Затраты

Китай — исходная версия. Денег не требуется. Сообщите об уязвимости поставщику продукта или через официальную платформу. Пока производитель не исправит уязвимость, не публикуйте ни детали, ни код для её проверки

Выгода

Китай — исходная версия. Эти правила распространяются на три категории: поставщиков сетевых продуктов на территории Китая, операторов сетей, а также

организации и частных лиц, которые занимаются обнаружением, сбором, публикацией сведений об уязвимостях и другой подобной деятельностью. Никаким организациям и частным лицам нельзя использовать уязвимости для действий, угрожающих безопасности сетей, а также незаконно собирать, продавать и публиковать сведения об уязвимостях. При публичном распространении сведений об уязвимостях нужно соблюдать пять правил. Первое: нельзя публиковать сведения, пока поставщик продукта не предоставит меры по исправлению. Второе: нельзя публиковать подробности об уязвимостях сетей, информационных систем и их оборудования, которые операторы сетей используют в данный момент. Третье: нельзя намеренно преувеличивать вред и риски, использовать сведения об уязвимостях для злонамеренного раздувания ажиотажа или мошенничества. Четвёртое: нельзя публиковать или предоставлять программы и инструменты, специально предназначенные для использования уязвимостей в действиях, угрожающих безопасности сетей. Пятое: при публикации нужно одновременно публиковать меры по исправлению или предотвращению угроз. Кроме того, неопубликованные сведения об уязвимостях нельзя предоставлять организациям или частным лицам за рубежом, кроме поставщика продукта. Правила поощряют сообщение об уязвимостях через четыре официальные платформы. Первая — Платформа обмена информацией об угрозах сетевой безопасности и уязвимостях Министерства промышленности и информатизации КНР (工业和信息化部网络安全威胁和漏洞信息共享平台). Вторая — Платформа уязвимостей Национального центра уведомлений о сетевой и информационной безопасности КНР (国家网络与信息安全信息通报中心漏洞平台). Третья — Платформа уязвимостей Национального координационного центра экстренного технического реагирования в компьютерных сетях КНР (国家计算机网络应急技术处理协调中心漏洞平台). Четвёртая — База уязвимостей Китайского центра оценки информационной безопасности (中国信息安全测评中心漏洞库). При сборе или публикации сведений об уязвимостях с нарушением правил Министерство промышленности и информатизации КНР (工业和信息化部) и Министерство общественной безопасности КНР (公安部) принимают меры по закону, каждое в пределах своих полномочий. Если нарушение подпадает под случаи, предусмотренные Законом КНР о кибербезопасности (网络安全法), наказание назначается по этому закону. При публичном распространении сведений о сетевой безопасности, включая уязвимости систем, нужно соблюдать соответствующие государственные правила. При нарушении компетентные ведомства предписывают устранить нарушение, выносят предупреждение и могут назначить штраф от 10 тыс. юаней до 100 тыс. юаней включительно. При отказе устранить нарушение или при серьёзных обстоятельствах нарушения назначается

штраф от 100 тыс. юаней до 1000 тыс. юаней включительно. Также могут предписать приостановить соответствующую деятельность, приостановить работу для устранения нарушений, закрыть сайт или приложение. Могут также отозвать разрешение на соответствующую деятельность или лицензию на ведение хозяйственной деятельности. Непосредственно ответственные руководители и другие непосредственно ответственные лица получают штраф от 10 тыс. юаней до 100 тыс. юаней включительно (по всему Китаю)

Примечания

Китай — исходная версия. Правила прямо включают частных лиц в круг тех, на кого они распространяются. «Я всего лишь любитель» не входит в число исключений. Передача сведений об уязвимостях систем в Китае зарубежным платформам вознаграждения за обнаружение уязвимостей прямо подпадает под положение «неопубликованные сведения об уязвимостях нельзя предоставлять за рубеж». Есть ли право проводить проверку — см. пункт 9 (без письменного разрешения не проверяйте чужие системы), а что делать после обнаружения уязвимости — это отдельный вопрос. Даже за законно обнаруженную уязвимость можно получить штраф, если способ публикации нарушает правила. Если уязвимость обнаружена при проверке без разрешения, проблемы есть с обеих сторон: и с проверкой, и с публикацией. Среди каналов сообщения чаще всего используются платформа Министерства промышленности и информатизации КНР (工信部) и Национальный центр экстренного реагирования в интернете КНР (国家互联网应急中心, CNCERT). Правила отдельно не выделяют ситуацию «производителя уже уведомили, но он не исправляет уязвимость». На практике сохраняют записи переговоров и сообщений об уязвимости и одновременно сообщают о ней через официальную платформу.

Источники

Китай — исходная версия — источники

- 1.工业和信息化部、国家互联网信息办公室、公安部 (2021). 网络产品安全漏洞管理规定 (工信部联网安〔2021〕66号, 第二、四、九、十、十四条, 2021年9月1日施行).
www.gov.cn/gongbao/content/2021/content_5641351.htm
- 2.全国人大常委会 (2025). 网络安全法 (2025年修正, 2026年1月1日施行, 第二十八、六十五条; 2016年文本为第二十六、六十二条, 规定第十四条援引的是2016年文本的条号).
www.cac.gov.cn/2025-12/29/c_1768735112911946.htm

