НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

Рекомендации по компенсации ИТ-рисков для компаний и организаций Российской Федерации в условиях санкционных ограничений

ALRT-20220319.1 | 19 марта 2022 г.

TLP: WHITE

Описание	В настоящее время продолжает расти угроза введения новых санкционных ограничений в отношении различных коммерческих и государственных организаций Российской Федерации, что влечет за собой появление новых ИТ-рисков, следствием которых может стать нарушение функционирования или доступности информационных ресурсов, вывод из строя средств защиты информации и прочее. Кроме этого, появляется все больше свидетельств об устремлении части неблагонамеренных разработчиков свободно распространяемого программного обеспечения нанести вред ИТ-инфраструктуре российских компаний и организаций, а также обычным пользователям. Для этого злоумышленники вносят недокументированные изменения в разрабатываемое ими программное обеспечение, которое впоследствии может нести как просто деструктивный или меркантильный характер, так и вовлечь пользователя в осуществление вредоносной активности на различные российские информационные ресурсы. При текущем ландшафте угроз безопасности информации НКЦКИ предлагает воспользоваться следующими рекомендациями, направленными на компенсацию некоторых ИТ-рисков.
Рекомендации	1. Проверить, что инфраструктура (хостинг), на которых размещаются публичные ресурсы, находится на территории Российской Федерации. 2. В случае аренды вычислительных мощностей необходимо компенсировать риск, возникающий в случае отказа хостинга размещать публичный ресурс, имеющий отношение к компании, находящейся под санкциями. 3. Удостовериться, что используемые для корректной работы публичных ресурсов DNS-сервера размещены на территории Российской Федерации. Также убедиться в отсутствии в цепочке серверов различных публичных иностранных серверов, например, DNS forwarding 8.8.8.8. 4. Убедиться, что регистратор, который управляет доменными именами публичных ресурсов, находится в Российской Федерации. В противном случае передать управление доменными именами любому отечественному регистратору. 5. В случае использования для публичных ресурсов основных доменных зон .com, .org и прочих, следует рассмотреть вариант преимущественного использования доменной зоны .ru. 6. При наличии собственной автономной системы (AS) проработать вопрос ее связности. 7. Провести ревизию SSL-сертификатов, разработать план по переходу на самоподписанные сертификаты или выпущенные удостоверяющими центрами, находящимися на территории Российской Федерации.

8. Организовать инвентаризацию облачных решений и разработать план по переходу на российские аналоги или решения, разворачиваемые локально и неконтролируемые производителем извне. Это касается в том числе и решений, которые используются коммерческими предприятиями: мессенджеры, система управления взаимоотношениями с клиентами (CRM), средства коллективной работы, офисные пакеты, интегрированные среды разработки (IDE) и прочее.

9. Провести инвентаризацию продуктов, требующих проверку лицензии за рубежом. Предпринять меры по поиску альтернатив.

10. Создать локальные хранилища дистрибутивов программных продуктов и используемого в компании программного обеспечения с открытым исходным кодом. Не обновлять его до последней версии, а в случае уже произведенного обновления откатиться к версиям продуктов, выпущенных ранее 24 февраля 2022 года. В случае если обновление необходимо, по возможности, устанавливать его только после проверки в тестовой среде.

11. Минимизировать использование или полностью запретить пользователям использовать стороннее программное обеспечение с открытым исходным кодом, если в этом отсутствует прямая необходимость.

12. В случае если в ИТ-инфраструктуре используются комплексные программные решения отечественного производства, в состав которых входит программное обеспечение с открытым исходным кодом, проработать мероприятия по его безопасному обновлению, по возможности, совместно с разработчиком такого решения.

13. Оценить финансовые взаимодействия с контрагентами и выявить компании, которые не смогут принимать платежи с территории Российской Федерации и потенциально могут отказаться от дальнейшего сотрудничества.