ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ (ФСТЭК России)

Старая Басманная, д. 17, Москва, 105066
Тел., факс: (495) 696-49-04
E-mail: postin@fstec.ru

24.03.2022 № 240/22/1549

На №_____

Организациям — разработчикам программного обеспечения и оборудования автоматизированных систем управления производственными и технологическими процессами

О мерах по повышению защищенности информационной инфраструктуры

Анализ сведений об угрозах безопасности информации, проводимый специалистами ФСТЭК России в условиях сложившейся обстановки, показывает, что зарубежными хакерскими группировками ведется подготовка и осуществляются масштабные компьютерные атаки на информационную инфраструктуру организаций-разработчиков разработчиков программного обеспечения и оборудования автоматизированных систем управления производственными и технологическими процессами, применяемых на объектах критической информационной инфраструктуры Российской Федерации программного обеспечения.

В целях обеспечения безопасности информации и повышения защищенности информационных инфраструктур организаций, используемых для разработки, поставки, распространения и технической поддержки программного обеспечения и оборудования автоматизированных систем управления производственными и технологическими процессами (далее – информационная инфраструктура), рекомендуется принять следующие дополнительные меры по повышению их защищенности:

провести инвентаризацию общедоступных информационных ресурсов (веб-сайтов, порталов) путем внешнего сканирования блока публичных IP-адресов, принадлежащих организации с целью определения сетевых служб открытых на периметре информационной инфраструктуры, а также путем сканирования IP-

адресов, выделенных для информационных ресурсов организации в арендованном облаке/хостинге, и отключить неиспользуемые службы и веб-сервисы;

по результатам сканирования провести анализ открытых портов и заблокировать доступ извне к сетевым службам, для которых он не нужен или ограничить доступ по белому списку IP-адресов там, где это возможно исходя из назначения сервиса;

для взаимодействия по интерфейсу API, если возможно, ограничить доступ по белому списку IP-адресов;

усилить требования к парольной политике администраторов и пользователей (потребителей) веб-сервисов организаций, исключив при этом использование паролей, заданных по умолчанию, а также отключить неиспользуемые учетные записи;

обеспечить двухфакторную аутентификацию сотрудников организации, осуществляющих удаленное подключение к информационной инфраструктуре;

обеспечить реализацию удаленного доступа сотрудников организации к инфраструктуре с применением средств удаленной дистанционной работы (при возможности) через защищенные каналы передачи данных (с применением протоколов HTTPS, SSH и других протоколов) с использованием VPN-сетей;

при невозможности исключения удаленной технической поддержки для потребителей обеспечить реализацию такой технической поддержки с использованием VPN-сетей и двухфакторной аутентификации;

исключить из публичного доступа информацию и материалы, содержащие сведения по настройке и эксплуатации программного обеспечения и оборудования, автоматизированных систем управления производственными и технологическими процессами, дистрибутивы и демо-версии программного обеспечения, размещаемых на сайтах организаций;

обеспечить фильтрацию трафика прикладного уровня с применением средств межсетевого экранирования уровня приложений (web application firewall (WAF)), установленных в режим противодействия атакам;

на сетевом оборудовании при наличии технической возможности отказаться от использование незащищенных протоколов управления, таких как telnet/http/snm, и разрешить доступ к оборудованию только из доверенных сетей (сегменты управления, рабочие станции администраторов);

активировать функции защиты от атак отказа в обслуживании (DDoS-атак) на средствах межсетевого экранирования и других средствах защиты информации.

Заместитель директора В.Лютиков