РЕКОМЕНДАЦИИ
по повышению защищенности информационной инфраструктуры Алтайского края

В целях повышения защищенности информационных систем органов исполнительной власти, органов местного самоуправления Алтайского края, а также подведомственных им организаций (далее – «государственные органы») рекомендуется:

приостановить работы по обновлению применяемого в информационных системах иностранного программного обеспечения и программно-аппаратных средств, страной происхождения которых является США и страны Европейского союза, а также исключить их автоматическое централизованное обновление посредством сети «Интернет».

В целях повышения защищенности официальных сайтов государственных органов рекомендуется:

усилить требования к парольной политике администраторов и пользователей сайтов государственных органов, исключив при этом использование паролей, заданных по умолчанию, отключить сервисные и неиспользуемые учетные записи;

провести инвентаризацию служб и веб-сервисов, используемых для функционирования официальных сайтов государственных органов (далее – «службы и веб-сервисы»);

обновить службы и веб-сервисы, функционирующие на периметре информационной инфраструктуры;

отключить неиспользуемые службы и веб-сервисы;

обеспечить поддержку сайтами государственных органов соединения с применением защищенных протоколов сетевого взаимодействия (HTTPS, SSH и других протоколов). Рекомендуется использовать только актуальные версии таких протоколов. Также не рекомендуется использовать ссылки на сайты с заголовками HTTP даже в теле страниц веб-приложения, поскольку при переходе по такой ссылке есть риск перехвата файлов cookie пользователей;

обеспечить фильтрацию сетевого трафика с целью исключения возможности подключения внешних пользователей к TCP-интерфейсам систем управления базами данных и интерфейсам удаленного управления компонентами сайтов. Рекомендуется оставлять доступными для подключения внешних пользователей только веб-интерфейсы 443/TCP (HTTPS) и 80/TCP (с принудительным перенаправлением на порт 443/TCP с HTTPS);

исключить возможность применения на сайтах государственных органов сервисов подсчета сбора данных о посетителях, сервисов предоставления информации о месторасположении и иных сервисов, разработанных иностранными организациями (например, сервисов onthe.io, ReCAPTCHA, YouTube, Google Analytics, Google Maps, Google Translate, Google Analytics);

исключить возможность использования встроенных видео- и аудио-файлов, интерфейсов взаимодействия API, «виджетов» и других ресурсов, загружаемых со сторонних сайтов, заменив их при необходимости гиперссылкой на такие ресурсы.

В целях повышения устойчивости сайтов государственных органов к распределенным атакам, направленным на отказ в обслуживании (DDoS-атакам) необходимо принять следующие первоочередные меры защиты информации (при наличии технической возможности):

обеспечить настройку правил средств межсетевого экранирования на блокировку не разрешенного входящего трафика;

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

активировать функции защиты от DDoS-атак на средствах межсетевого экранирования и других средствах защиты информации;

ограничить количество подключений с каждого IP-адреса (например, установить на веб-сервере параметр raid-limit);

блокировать входящий трафик, поступающий с IP-адресов, страной происхождения которых являются США, страны Европейского союза или иной страной, являющейся источником компьютерных атак;

блокировать трафик, поступающий из «теневого Интернета» (сети Tor) (список узлов, которые необходимо заблокировать, содержатся по адресу: https://www.dan.me.uk/tornodes);

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