Перечень организационно-технических мер по повышению защищенности объектов[1] информационной инфраструктуры

1. Первоочередные[2] организационно-технические меры:

1) провести инвентаризацию служб и веб-сервисов, используемых для функционирования информационных систем и ресурсов включая официальные сайты (далее- – ИСР) и размещенных на периметре информационной инфраструктуры (далее – службы и веб-сервисы);

2) отключить неиспользуемые службы и веб-сервисы;

3) усилить требования к парольной политике администраторов и пользователей ИСР, исключив при этом использование паролей, заданных по умолчанию, отключить сервисные и неиспользуемые учетные записи;

4) обеспечить сетевое взаимодействие с применением защищенных актуальных версий протоколов сетевого взаимодействия (HTTPS, SSH и других протоколов);

5) исключить применение в ИСР подсчета и сбора данных о посетителях, сервисов предоставления информации о местоположении и иных сервисов, разработанных иностранными организациями (например, сервисов onthe.io, ReCAPTCHA, YouTube, Google Analytics, Google Maps, Google Translate, Google Analytics);

6) 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;

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

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

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

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

11) провести выявление возможных точек проникновения внешнего нарушителя на объекты информационной инфраструктуры **[3]** (далее – ИИ) (каналы удаленного доступа, подключения к информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»), через взаимодействие с иными информационными (автоматизированными) системами, через беспроводные сети, через веб-интерфейсы и другие способы проникновения);

12) ограничить доступ через выявленные точки проникновения, в том числе ограничение удаленного к объектам ИИ подключения к объектам и подключение к сети «Интернет»;

13) проанализировать уязвимость узлов объектов ИИ, являющихся точками проникновения внешнего нарушителя на объекты ИИ, в том числе уязвимостей конфигурации и кода программного обеспечения узлов включая прикладное

и системное программное обеспечение, прошивки оборудования;

14) принять меры по устранению критических уязвимостей узлов объектов ИИ, являющихся точками проникновения внешнего нарушителя на объекты ИИ;

15) проинформировать администраторов и пользователей информационных систем о недопущении распространения информации о функционировании информационной системы, передаче сторонним лицам своей аутентификационной информации;

16) проинформировать администраторов и пользователей информационных систем об ответственности за нарушение требований в области информационной безопасности;

17) провести смену аутентификаторов учетных записей пользователей программного обеспечения, установленного на соответствующих узлах сети;

18) ограничение возможности удаленного управления прикладным и системным программным обеспечением, системным программным телекоммуникационным оборудованием через сеть «Интернет»;

19) исключить применение иностранных систем видеоконференции,

в том числе Zoom, Skype, а также систем удаленного доступа (RAdmin, TeamViewer, AnyDesk);

20) обеспечить регистрацию событий безопасности информации, особенно событий, связанных с внешними подключениями к объектам ИИ, сетевого трафика, превышением количества пользователей в системы, с попытками запуска сторонних программ и анализом попыток входа сервисов, а также с удаленным доступом.

2. Дополнительные[4] организационно-технические меры:

1) провести проверку настроек средств межсетевого экранирования и активного сетевого оборудования, находящегося на границе периметра объекта ИИ, включая актуальные обновления прошивок, отключение неиспользуемых портов и ограничение на доступ пользователей в сеть «Интернет»;

2) провести проверку наличия вредоносного программного обеспечения поступающих незапрашиваемых электронных сообщениях (письмах, документах);

3) реализовать настройку многофакторной аутентификации для удаленного и локального доступа привилегированных пользователей объектов ИИ;

4) осуществлять контроль невозможности подключения неучтенных съемных машинных носителей информации и мобильных устройств;

6) проводить проверку актуальности версий программного обеспечения средств защиты информации, применяемых для обеспечения безопасности объектов ИИ,

а также их баз данных, осуществляемая не реже, чем раз в 3 дня, при наличии

их обновлений незамедлительное применение этих обновлений;

8) организовать проверку соблюдения ограничений на использование на объектах ИИ личных средств вычислительной техники (ноутбуков, планшетов, смартфонов), модемов и съемных машинных носителей информации и правил безопасного использования таких средств;

9) организовать проверку соблюдения ограничений на применение на объектах ИИ наиболее часто используемого при реализации компьютерных атак программного обеспечения, в том числе Microsoft Office, Adobe, Autocad, браузеров, средств администрирования командных оболочек (например, PowerShell, Bash и другие) и правил их безопасного использования;

10) организовать проверку на объектах ИИ соблюдения ограничений на использование программного обеспечения, не относящегося к производственной деятельности и не требуемого для выполнения должностных обязанностей работников объектов ИИ;

11) информировать работников объектов ИИ, поставщиков продуктов и услуг в сфере информационных технологий, подрядных организаций в сфере информационных технологий, иных юридических лиц, имеющих доступ к объектам ИИ, о необходимости принятия мер по блокированию угроз и о необходимости соблюдения требований по безопасности при предоставлении услуг.

---

[1] С учетом особенностей функционирования объектов информационной инфраструктуры.

[2] Рекомендуемое время реализации от момента поступления настоящего перечня-72 часа;

[3] Под объектами информационной инфраструктуры понимаются информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления.

[4] Рекомендуемое время реализации мероприятий от момента поступления настоящего перечня-120 часов