ФСТЭК РОССИИ
УПРАВЛЕНИЕ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ ПО ДАЛЬНЕВОСТОЧНОМУ ФЕДЕРАЛЬНОМУ ОКРУГУ
Ленина, д. 37, г. Хабаровск, 680030
Тел., факс (4212) 35-11-08
E-mail: dfo@fstec.ru

22.06.2022 г. № 2/1749

На № _____

Первому вице-губернатору
Хабаровского края,
председателю Совета по
информационной безопасности
при Губернаторе Хабаровского края
А.А.НИКИТИНУ

main@adm.khv.ru

О мерах по повышению защищенности информационной инфраструктуры Российской Федерации

Уважаемый Александр Александрович!

Анализ сведений об угрозах безопасности информации, проводимый специалистами ФСТЭК России в условиях сложившейся обстановки, показывает, что зарубежными хакерскими группировками в отношении федеральных органов исполнительной власти и организаций Российской Федерации (далее — органы (организации)) продолжают реализовываться успешные компьютерные атаки, направленные на получение защищаемой информации (конфиденциальной информации, персональных данных граждан и работников, конфигурационной информации об информационной инфраструктуре).

По результатам анализа сведений о происходящих с 24 февраля 2022 г. инцидентах безопасности информации установлено, что основными способами получения несанкционированного доступа к защищаемой информации являются:

подкуп работников органов (организаций) в целях получения защищаемой информации;

несанкционированный доступ к информационной инфраструктуре подрядных организаций и получение через него доступа к информационным системам органов (организаций);

эксплуатация уязвимостей в информационных системах органов (организаций).

С целью предотвращения утечки защищаемой информации за счет подкупа работников органов (организаций) необходимо принять следующие дополнительные меры защиты информации:

проинформировать администраторов и пользователей информационных систем об ответственности за нарушение требований в области информационной безопасности и разглашение конфиденциальной информации;

усилить контроль действий администраторов и пользователей, связанных с обработкой конфиденциальной информации в информационных системах;

провести внеплановую смену паролей администраторов и пользователей, используемых для доступа в информационные системы;

провести анализ учетных записей администраторов и пользователей информационных систем на предмет отсутствия незаблокированных учетных записей уволенных работников и наличия неизвестных учетных записей;

исключить (при возможности) удаленный доступ посредством сети «Интернет» к информационным системам для администраторов и пользователей;

обеспечить регистрацию и мониторинг событий безопасности в информационной системе;

минимизировать количество съемных машинных носителей информации, подключаемых к информационной системе;

при наличии систем предотвращения утечки информации (DLP-систем) обеспечить контроль содержимого файлов, передаваемых посредством электронной почты, съемных машинных носителей информации;

обеспечить мониторинг информационных ресурсов, расположенных в сети «Интернет», на предмет выявления сведений от утечках защищаемой информации органа (организации) и оперативное принятие мер по предотвращению ущерба от таких утечек.

С целью предотвращения утечки защищаемой информации через взлом информационной инфраструктуры подрядной организации необходимо принять следующие дополнительные меры:

определить в рамках договорных отношений ответственность подрядных организаций за защиту информации при реализации удаленного доступа к информационной системе;

определить перечень работников подрядных организаций, для которых предполагается удаленный доступ к информационной инфраструктуре;

определить перечень информации и информационных ресурсов, расположенных на серверах информационных систем, к которым будет предоставляться удаленный доступ работникам подрядных организаций;

предоставить учетные записи работникам подрядных организаций для доступа в информационную систему с минимально необходимыми правами доступа;

осуществлять мониторинг действий работников подрядных организаций;

выделить в отдельный домен работников подрядных организаций, управление которого должно осуществляться с серверов информационных систем;

обеспечить защищенный удаленный доступ работников подрядной организации к информационной инфраструктуре с применением сертифицированных по требованиям безопасности информации средств обеспечения безопасной дистанционной работы в информационных (автоматизированных) системах;

обеспечить подключение подрядных организаций с выделенных автоматизированных рабочих мест, не имеющих сторонних подключений к другим организациям;

регламентировать подключение подрядных организаций путем введения согласования каждого удаленного подключения и ограничения времени, в течение которого оно выполняется (при возможности).

С целью предотвращения утечки защищаемой информации через эксплуатацию уязвимостей информационных систем органов (организаций) необходимо принять следующие дополнительные меры:

провести инвентаризацию информационных ресурсов, расположенных на периметре, путем внешнего сканирования публичных IP-адресов, принадлежащих органу (организации);

отключить неиспользуемые службы и веб-сервисы, выявленные по результатам сканирования;

провести внеплановый анализ уязвимостей служб и веб-сервисов, по результатам которого принять меры по недопущению эксплуатации критических уязвимостей.

С уважением,

Исполняющий обязанности
руководителя Управления Р.Хабибулин