Рекомендации по безопасности информации от несанкционированного доступа к защищаемой информации

1.По результатам анализа сведений о происходящих с февраля 2022 года 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 0б 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, осуществляющей мероприятия по защите информации, 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.

2. Повышение защищенности информационной инфраструктуры Российской Федерации и устойчивости ее функционирования к распределенным атакам, направленным на отказ в обслуживании (DDoS-атак), рекомендуется принять следующие меры защиты информации:

-по возможности осуществить «эшелонированный» подход к защите от DDoS-атак, который заключается в разграничении фильтрации трафика между провайдером (на канальном уровне) и государственным органом (организацией), принимающим трафик (на прикладном уровне);

-по возможности использовать технологию сетей доставки содержимого (CDN-технологии), которые заключаются в использовании географически распределенной сетевой инфраструктуры, позволяющей оптимизировать доставку и дистрибуцию содержимого конечным пользователям;

-использовать сетевое оборудование (маршрутизаторы), обладающее специализированными аппаратными решениями, которые отвечают за пакетную обработку на максимальной скорости на пакетах малой длины и поддерживает максимальную скорость передачи данных физического уровня (wirespeed-обработка);

-обеспечить защиту от атак на таблицу состояний (например, отправки большого количества запросов на подключение по протоколу управления передачей (TCP-протокола) при использовании технологий синхронизации прокси (SYN Proxy) и ограничения по количеству одновременных соединений с одного IP-адреса;

-по возможности использовать серверное оборудование для управления балансировщиками нагрузки или межсетевыми экранами, способное выдержать большие нагрузки при обработке TLS-трафика прикладных запросов;

-не размещать в одной сети передачи данных общедоступные ресурсы государственных органов (организаций) и ресурсы, обеспечивающие выход работников в сеть «Интернет»;

-по возможности организовывать выход работников государственного органа (организации) в сеть «Интернет» по каналам связи, адресное пространство которых сложно ассоциировать с государственными органами (организации);

-для управления серверами информационной инфраструктуры государственных органов (организаций) использовать сетевые интерфейсы, отличные от интерфейсов передачи данных;

-при необходимости размещать общедоступные ресурсы государственных органов и организаций во внешнем облаке провайдера;

-использовать хостинг доменных зон у соответствующих провайдеров для защиты службы доменных имен (DNS-служба) или услуги по защите DDoS-атак от специализированного провайдера;

-по возможности отказаться от размещения в общедоступных ресурсах сервисов, используемых государственным органом (организацией), которые работают по протоколу пользовательских датаграмм (UPD-протоколу) или осуществить их перевод на работу по протоколу управления передачей (TCP-протоколу);

-проводить регулярную инвентаризацию общедоступного IP-адресного пространства, включая неиспользуемые IP-адреса сайтов государственного органа (организации) с целью современного реагирования на подмену или компрометацию указанного адресного пространства;

-по возможности вывести все сервисы, используемое государственным органом (организацией), которые работают по протоколу пользовательских датаграмм (UPD-протоколу) в отдельную подсеть;

-произвести настройку межсетевых экранов в части сокращения таймаутов для соединений, работающих по протоколу управления передачей (TCP-протоколу).