Рекомендации по защите информации по повышению защищенности информационных систем и информационно-телекоммуникационных сетей органов государственной власти

1. Меры защиты информации в ИС и ИТКС:

1.1. 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 систем и сетей, а также путем сканирования IP-адресов, выделенных для систем и сетей организации в арендованном облаке/хостинге, и отключить неиспользуемые службы и веб-сервисы.

1.2. По результатам сканирования провести анализ открытых портов, определить принадлежность и легитимность доступных по открытым портам сервисов и заблокировать доступ извне к сетевым службам, для которых он не требуется или ограничить доступ по белому списку IP-адресов там, где это возможно исходя из назначения сервиса. Инвентаризация должна проводиться на периодической основе, но не реже раза в квартал.

1.3. Выявить все поддоменны, зарегистрированные в домене организации путем анализа мастер-зоны на авторитативном DNS-сервере, и провести инвентаризацию IP-адресов всех поддоменов.

1.4. Провести инвентаризацию систем и сетей на предмет наличия отдельных каналов управления программным обеспечением и оборудованием. Например, какие каналы строятся с использованием 3G/LTE оборудования и расширяют поверхность реализации компьютерных атак.

В условиях отсутствия технической возможности реализации мер защиты информации для подобных решений, необходимо произвести учет всех устройств, провести сканирование их IP-адресов, устранить критические уязвимости, закрыть открытые порты и сменить пароли. В случае невозможности устранения уязвимостей рассмотреть возможность отключения каналов управления.

1.5. Обеспечить доступ к внутренним сервисам организации посредством виртуальных частных сетей (VPN) с использованием двухфакторной аутентификации. При возможности реализовать следующий набор ограничений:

удаленный доступ работников осуществлять только с IP-адресов, закрепленных за автономными системами Российской Федерации;

при необходимости доступа с зарубежных IP-адресов реализовать ограничение по белому списку;

разработать правила корреляции в системах мониторинга информационной безопасности (SIEM) по подключениям с иностранных IP-адресов;

блокировать подключения к информационным системам с IP-адресов VPN-провайдеров, узлов TOR и подсетей хостеров (hetzner, qhoster и других подсетей);

запретить удаленное администрирование с подключением с зарубежных IP-адресов.

1.6. В случае наличия на периметре систем и сетей почтовых сервисов (включая сервисы OWA), сервисов файлового обмена (таких как FTP), реализовать меры, указанные в пункте 1.5 настоящего документа.

1.7. Для взаимодействия с приложением по интерфейсу API ограничить доступ по белому списку IP-адресов (при возможности).

1.8. При наличии собственной автономной системы (AS) и блока публичных IP-адресов, организовать мониторинг атак типа BGP Hijack с использованием сервиса от оператора связи или специализированного отечественного сервис провайдера (при возможности).

1.9. Перейти на использование услуг доступа к сети «Интернет» и телефонии у российских операторов связи (при возможности).

1.10.Организовать подключение своей автономной системы к MSK-IX (при возможности).

1.11.Обеспечить защиту критичных веб-ресурсов с помощью фильтрации трафика прикладного уровня с применением средств межсетевого экранирования уровня приложений (web application firewall (WAF)), установленных в режим противодействия атакам, и защиты от атак отказа в обслуживании (DDoS-атак) на средствах межсетевого экранирования и других средствах защиты информации.

1.12.Убедиться, что критичные веб-приложения и веб-ресурсы, которые необходимы для осуществления основных процессов, а также основные веб--ресурсы не содержат компонентов, подгружаемых с внешних неконтролируемых ресурсов. В случае выявления такого кода, рассмотреть возможность временного или постоянного его отключения.

1.13.На сетевом оборудовании при наличии технической возможности отказаться от использования незащищенных протоколов управления, таких как telnet/http/snmp, и разрешить доступ к оборудованию только из доверенных сетей (сегменты управления, рабочие станции администраторов).

1.14.Ограничить использование обезличенных учетных записей на сетевом оборудовании.

1.15.В случае необходимости использования SNMP для мониторинга и/или управления оборудованием, ограничить к нему доступ путем изоляции на уровне VLAN/VRF, а также применения ACL для доверенного списка адресов. При этом необходимо отказаться от применения snmp-community по умолчанию (public, private) и использовать SNMP v.3.

1.16.В случае применения в системах и сетях AAA серверов, провести настройку сетевого оборудования на централизованную аутентификацию по TACACS+, RADIUS, или LDAP.

1.17.В случае использования зарубежных публичных NTP-серверов перейти на использование публичного NTP-сервера MSK-IX:

Имя сервера	ntp.msk-ix.ru
1Ру4-адрес	194.190.168.1
1Ру6-адрес	2001:6d0:ffd4::1

1.18.В случае использования зарубежных CDN провайдеров, в том числе Akamai, CloudFlare, необходимо перейти на использование отечественных аналогов.

1.19.Организовать хостинг ресурсов на территории Российской Федерации. При ведении международной деятельности при необходимости возможно организовать зеркало сайта на хостинге за рубежом.

1.20.Реализовать защищённый доступ пользователей к веб-ресурсам сети

«Интернет» через шлюзы или прокси-сервера (при возможности) с использованием:

функций потокового антивируса (для антивирусной проверки всего загружаемого контента), обнаружения вторжений (для предотвращения попыток эксплуатации уязвимостей клиентских приложений), фильтрации URL-адресов и веб-приложений;

функции интеграции с «песочницей», выполняющей открытие в изолированном окружении всех загружаемых из сети «Интернет» файлов для анализа их потенциального воздействия на систему;

ограничения доступа к зарубежным ресурсам, за исключением тех, которые необходимы по работе, или разрешения доступа к ресурсам из белого списка IP-адресов (при возможности).

1.21.Использовать DNS-сервера на территории Российской Федерации:
авторитативные - для хостинга зоны использовать несколько провайдеров

с обязательной защитой от DDoS-атак;

рекурсивные - использовать DNS от оператора связи и/или специализированных российских провайдеров 014$, и/или Национальной системы доменных имен (НСДИ);

в случае ведения международной деятельности организовать хостинг зоны в том числе у зарубежных провайдеров;

если организация использует домен не в зоне .RU, .РФ, .SU, необходимо закупить домен в зоне .RU и обеспечить работоспособность ресурсов.

1.22. Обеспечить наличие у организации прав на свои доменные имена.

1.23. Обеспечить разнесение ролей DNS-серверов «User Primary DNS Server»[1] и «Domain Primary DNS Server»[2] на разные физические и (или) виртуальные серверы.

1.24. В части «Domain Primary DNS Server»:

запретить рекурсивные запросы разрешения доменных имен;

запретить разрешение доменных имен объектов, не относящихся к информационным ресурсам организации;

настроить механизмы защиты от спуфинг-атак;

запретить уведомления и перенос зон произвольными объектами сети Интернет. Настроить список доверенных DNS-серверов;

настроить правила предварительной фильтрации поступающих запросов (Таблица №1).

Таблица № 1: Правила фильтрации запросов.

Описание	**IP-адрес очника**	**Сетевой порт очника**	**IP-адрес начения**	**Сетевой порт начения**
Входящий запрос	Любой	53/udp; 53/tcp; >1023/udp; >1023/tcp.	IP-адрес DNS-сервера	53/udp; 53/tcp.
Ответ на запрос	IP-адрес DNS-сервера	53/udp; 53/tcp.	Любой	53/udp; 53/tcp; >1023/udp; >1023/tcp.

1.25. Запретить в качестве «User Primary DNS Server» использовать DNS-серверы, расположенные за пределами Российской Федерации (например, перейти на использование национальной системы доменных имен).

1. User Primary DNS Server – DNS-сервер, отвечающий на запросы пользователей информационных ресурсов организации по разрешению доменных имен объектов сети Интернет.
2. Domain Primary DNS Server - DNS-сервер, отвечающий на запросы пользователей сети Интернет и других DNS-серверов по разрешению доменных имен, принадлежащих информационным ресурсам организации.

2. Меры защиты систем и сетей при работе с подрядными организациями, поставщиками услуг в сфере информационно-телекоммуникационных технологий

2.1. Обеспечить управлением сетевым доступом в точках сопряжения с сетями сторонних организаций.

2.2. Использовать системы обнаружения вторжений или решений класса Network Traffic Analysis (NTA) в точках сопряжения с сетями подрядных организаций и поставщиков услуг, позволяющих блокировать известные компьютерные атаки и выполнять непрерывную запись метаданных сетевого трафика для выявления потенциальных аномалий.

2.3. Для пользовательских подключений из сети подрядных организаций, поставщиков услуг использовать персонифицированные учетные записи с двухфакторной аутентификацией.

2.4. Обеспечить реализацию удаленного доступа сотрудников подрядных организаций и поставщиков услуг к системам и сетям с применением средств удаленной дистанционной работы (при возможности) через защищенные каналы передачи данных (с применением протоколов HTTPS, SSH и других протоколов).

2.5. Обеспечить управление учётными записями для сотрудников сторонних организаций по принципу минимальных привилегий.

2.6. По возможности реализовать контроль действий сотрудников подрядных организаций и поставщиков услуг с возможностью экстренного отключения сессии сотрудника и откатом его действий (должна быть реализована запись его действий).