АДМИНИСТРАЦИЯ
ВАСИЛЕОСТРОВСКОГО РАЙОНА
САНКТ-ПЕТЕРБУРГА

Государственное бюджетное общеобразовательное учреждение средняя общеобразовательная школа № 17 Василеостровского района Санкт-Петербурга

Санкт-Петербург, 19 линия, дом 22
Телефон/Факс: (812) 417-62-93
E-mail: school17vo@mail.ru
ОКПО 52153687, ОКОГУ 23280,
ОГРН 1037800062585,
ИНН 7801136782, КПП 780101001

ПРИКАЗ

15.04.2022 г. № 22/1-ОД

«О назначении ответственного лица за защиту ИТС»

В соответствии с письмом Минпросвещения РФ от 03.03.2022 г. № 04-147 «О мерах по повышению защищенности информационной инфраструктуры системы образования», с целью предотвращения получения зарубежными хакерскими группировками информации об особенностях функционирования информационных систем в образовательном учреждении

ПРИКАЗЫВАЮ:

1. Назначить с 15.04.2022 г. зам. директора по ШИС Громова В.В. ответственным за повышение защищенности периметра информационных систем и обеспечение безопасности информационно-телекоммуникационных сетей в ГБОУ СОШ № 17.
2. Зам. директора по ШИС Громову В.В. принять дополнительные меры по следующим направлениям работ:

2.1. проинформировать администраторов и пользователей информационных систем о недопущении распространения информации о функционировании информационной системы, передаче сторонним лицам своей аутентификационной информации;
2.2. проинформировать администраторов и пользователей информационных систем об ответственности за нарушение требований в области информационной безопасности;
2.3. усилить контроль над действиями в информационной системе администраторов и пользователей;
2.4. провести внеплановую смену паролей администраторов и пользователей, используемых для доступа в информационные системы;
2.5. исключить удаленный доступ посредством сети «Интернет» к информационным системам для администраторов и пользователей;
2.6. обеспечить двухфакторную аутентификацию администраторов информационных систем.

3. Зам. директора по ШИС Громову В.В. 25.04.2022 г. провести инструктаж с сотрудниками ГБОУ СОШ № 17.
4. Зам. директора по ШИС Громову В.В. при выполнении вышеуказанных поручений руководствоваться «Обобщенным перечнем мер защиты информации информационной инфраструктуры органов государственной власти и организаций РФ» (Приложение 1).

5. Контроль за исполнением настоящего приказа оставляю за собой.

Директор Т.И.Григорьева

С приказом ознакомлен и согласен:

ФИО	Подпись	Дата
Громов В.В.		

Приложение 1

Обобщенный перечень мер защиты информации информационной инфраструктуры органов государственной власти и организаций Российской Федерации

1. Меры защиты информации по повышению защищенности периметра информационных систем и информационно-телекоммуникационных сетей органов государственной власти и организаций Российской Федерации (далее - системы и сети)

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::l

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 DNS, 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.

2. Меры защиты систем и сетей, функционирующих под управлением операционных систем Microsoft Windows

2.1. Меры защиты информации от угроз безопасности информации, направленных на получение учётных данных пользователей путём их извлечения из памяти или различных системных хранилищ.

2.1.1. Минимизировать использование неподдерживаемых версий операционных систем Microsoft Windows (включая устаревшие версии Windows 10). Убедиться, что на всех автоматизированных рабочих местах под управлением Windows 7/Windows 8/Windows Server 2008 R2/Windows Server 2012, где по каким-либо причинам невозможен переход на более новые версии ОС, установлено обновление KB2871997 (https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/the-importance-of-kb2871997-and-kb2928120-for-credential/ba-p/2 58478).

2.1.2. Убедиться, что на всех доменных автоматизированных рабочих местах для провайдера аутентификации WDigest отключено кеширование паролей интерактивно аутентифицировавшихся пользователей в открытом виде в памяти процесса Lsass (https://docs.microsoft.com/en-us/answers/questions/463368/disabling-credentials-caching-in-wdigest.html). Использовать групповую политику для принудительного отключения данного кеширования, а также реализовать мониторинг изменений отвечающего за данную настройку ключа реестра.

2.1.3. Включить на всех доменных автоматизированных рабочих местах принудительную очистку памяти от учётных данных при выходе пользователя из системы путём установки значения ключа реестра, отвечающего за данную настройку (https://support.microsoft.com/en-us/topic/microsoft-security-advisory-update-to-improve-credentials-protection-and-management-may-13-2014-9343425l-04ac-b7f3-52aa-9f951cl4b649).

2.1.4. Запретить групповой политикой хранение в штатном менеджере паролей Windows учётных данных для сетевой аутентификации (https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-do-not-allow-storage-of-passwords-and-credentials-for-network-authentication).

2.1.5. По возможности использовать на всех доменных автоматизированных рабочих местах механизм LSA Protection для защиты памяти процесса lsass от доступа со стороны недоверенных процессов (https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection). Более эффективной альтернативой данному механизму является применение функционала защиты памяти процесса lsass в решениях по защите конечных точек. Например, механизм Credentials Guard, доступный в новых версиях операционных систем Windows (https://docs.microsoft.com/en-us/windows/security/identity-protection/ credential-guard/credential-guard).

2.1.6. Используя групповую политику, ограничить возможность использования привилегии отладки (SeDebugPrivilege) для административных учётных записей на всех доменных хостах (https://docs.microsoft.com/en-us/windows/security/threat-

protection/security-policy-settings/debug-programs). Если данная привилегия необходима для отдельных категорий пользователей (например, разработчиков), разрешить её только для данных учётных записей.

2.1.7. Отключить или ограничить кеширование учётных данных интерактивно вошедших пользователей, используемое для доступа в систему при недоступности контроллеров домена.

(https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-number-of-previous-logons-to-cache-in-case-domain- controller-is-not-available).

Для стационарных автоматизированных рабочих мест, имеющих постоянное подключение к системам и сетям, рекомендуется отключить кеширование, для мобильных автоматизированных рабочих мест минимизировать размер кеша до 1-2 записей.

2.2. Меры защиты информации, направленные на ограничение возможностей нарушителей по использованию полученных учётных данных для перемещения между автоматизированными рабочими местами сети организации.

2.2.1. Ограничить возможность сетевого доступа между автоматизированными рабочими местами по протоколам DCOM, SMB, RDP, WinRM. Данное ограничение может быть реализовано с использованием средств межсетевого экранирования, ACL на access-портах коммутаторов, Private VLAN, Wireless Client Isolation.

2.3. Меры защиты привилегированных учётных записей.

2.3.1. Использовать усиленные парольные политики для привилегированных учётных записей (более частая смена, повышенные требования к сложности пароля). Для реализации возможности использования различных парольных политик для разных категорий пользователей в Windows использовать механизм Fine-Grained Password Policies (https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc770394(v=ws.10).

2.3.2. Для защиты привилегированных учётных записей реализовать многоуровневую модель доступа, подразумевающую выделение как минимум следующих уровней:

Уровень 0: Контроллеры домена;

Уровень 1: Сервера;

Уровень 2: Рабочие станции.

2.3.3. Для администрирования каждого из уровней должны использоваться раздельные привилегированные учётные записи с применением групповой политики (параметры «Deny access to this computer from the network», «Deny logon locally», «Deny logon through Remote Desktop», «Deny logon as a batch job», «Deny logon as a service») рекомендуется реализовать следующие ограничения:

запрет входа под учётными записями уровня 0 на автоматизированные рабочие места уровней 1 и 2 (запрет входа под доменными администраторами на рабочие станции и сервера);

запрет входа под учётными записями уровня 1 на автоматизированные рабочие места уровней 2 (запрет входа под учётными записями администраторов серверов на рабочие станции).

Более подробные рекомендации по реализации многоуровневой модели возможно получить по ссылке:

https://docs.microsoft.com/en-us/security/compass/privileged-access-access-model.

2.3.4. Рекомендуется использовать выделенные физические или виртуальные автоматизированные рабочие места для администраторов с усиленными мерами по безопасности, подключенные к изолированному сетевому сегменту. Более подробные рекомендации по реализации данной меры возможно получить по ссылке https://docs.microsoft.com/en-us/security/compass/privileged-access-devices.

2.3.5. Для администрирования автоматизированных рабочих мест использовать штатную учётную запись локального администратора с уникальным паролем на каждой рабочей станции. Обеспечить регулярную смену паролей данных учётных записей,

используя механизм LAPS (https://www.microsoft.com/en-us/download/details.aspx?id=46899).

2.3.6. Использовать группу Protected Users для всех привилегированных доменных учётных записей, например, администраторов домена (https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group).

2.3.7. Запретить делегирование для всех привилегированных доменных учётных записей, например, администраторов домена (https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/active-directory-accounts#task4-disable-account-delegation).

2.3.8. Для безопасного удалённого администрирования операционных систем Windows с использованием RDP рекомендуется принять следующие меры:

исключить возможность доступа по RPD напрямую из сети «Интернет»;

включить обязательную аутентификацию на уровне сети (Network Level Authentication, https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.ll));

настроить автоматическое завершение сессий при отключении от удалённого рабочего стола без завершения сессии (https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc758177(v=ws.l0)?redirectedfrom=MSDN);

по возможности использовать Restricted Admin Mode (https://social.technet.microsoft.com/wiki/contents/articles/32905.remote-desktop-services-enable-restricted-admin-mode.aspx) или Windows Defender Remote Credential Guard (https://docs.microsoft.com/en-us/windows/security/identity-protection/remote-credential-guard).

2.3.9. Обеспечить регулярную (не реже одного раза в год) смену пароля сервисной учётной записи krbtgt. Также необходимо выполнить принудительную внеплановую смену пароля данной учётной записи в следующих ситуациях:

увольнение сотрудника, имевшего привилегии доменного администратора;

подозрение на компрометацию учётной записи с привилегиями доменного администратора.

Обращаем внимание, что из-за особенностей функционирования среды Active Directory для полной смены пароля krbtgt необходимо поменять его 2 раза подряд (https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/ad-forest-recovery-resetting-the-krbtgt-password).

2.3.10. Проводить регулярный аудит состава привилегированных групп. Обращаем внимание, что к привилегированным группам относятся: группы Domain Admins или Enterprise Admins, Administrators, Domain Admins, Enterprise Admins, Schema Admins, Account Operators, Print Operators, Server Operators, Domain Controllers, Read-only Domain Controllers, Enterprise Domain Controllers, Group Policy Creators Owners, DnsAdmins, Key Admins, Enterprise Key Admins, Organization Management, Exchange Trusted Subsystem, Exchange Windows Permissions.

2.4. Меры защиты сервисных учётных записей

2.4.1. Ограничить количество сервисных учётных записей с разрешённым неограниченным делегированием. По возможности использовать ограниченное делегирование вместо неограниченного (https://adsecurity.org/?p=1667).

2.4.2. Использовать стойкие пароли для сервисных учётных записей и осуществлять их регулярную смену (не реже раза в полгода или квартал). Для автоматизации регулярной смены паролей сервисных учётных записей рекомендуется использовать механизм gMSA (https://docs.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/getting-started-with-group-managed-service-accounts).

Также необходимо убедиться, что сервисные учётные записи не являются членами привилегированных доменных групп.

2.4.3. Используя групповые политики, рекомендуется ограничить возможность входа под сервисными учётными записями на автоматизированные рабочие места, где их использование недопустимо (например, интерактивный, RPD или сетевой вход под сервисной учётной записью на пользовательскую рабочую станцию).

2.4.4. Для администраторов автоматизированных рабочих мест и серверов рекомендуется заводить раздельные учетные записи (с правами обычного пользователя и с повышенными правами). Повседневная деятельность, не требующая повышенных привилегий, должна вестись с правами обычного пользователя.

2.5. Общесистемные меры защиты информации операционных систем Microsoft Windows.

2.5.1. Проводить регулярный аудит доменных учётных записей. Особое внимание обращать на следующие учётные записи:

не использовавшиеся длительное время;

длительное время не менявшие пароль;

учётные записи с включенными свойствами «Store password using reversible encryption», «Password Not Required», «Password Never Expires», «DES Kerberos Encryption Enabled», «Do not require Kerberos Pre-Authentication»;

учётные записи, ассоциированные с людьми (в особенности привилегированные), имеющие прописанные SPN, которые, как правило, указываются только для сервисных учётных записей, либо учётных записей компьютеров.

2.5.2. Отключить возможность добавления в домен новых автоматизированных рабочих мест непривилегированными пользователями. По умолчанию любой доменный пользователь имеет право на самостоятельное добавление в домен до 10 автоматизированных рабочих мест.

2.5.3. Включить на всех узлах расширенные политики аудита согласно уровню «Stronger Recommendation» (https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations).

2.5.4. Использовать политики «AppLocker» ограничения запуска исполняемых файлов по белому списку.

3. Меры защиты систем и сетей, функционирующих под управлением операционных систем на базе ядра Linux

3.1 Обеспечить аутентификацию по SSH-ключам, а также отключить возможность входа с правами «root» (повышение привилегий должно происходить посредством настройки политик sudo). Отключить прямой доступ по SSH из сети «Интернет».

3.2 Включить службу логирования auditd, а также осуществлять централизованный сбор и мониторинг событий, как минимум на выполнение команд: «sudo -1», «export HISTFILE=/dev/null», «unset HISTFILE», history -cw и тд., а также auth.log.

3.3 Осуществлять мониторинг выполнения команд для служебных (сервисных) учетных записей не типичных для служб, к которым они относятся.

3.4 Осуществлять сбор и мониторинг событий создания SSH-тоннелей и проброса портов.

3.5 Осуществлять сбор и мониторинг событий изменения файлов /etc/passwd, /etc/shadow.

3.6 Производить проверку контрольных сумм (md5/sha512) загружаемых и устанавливаемых файлов.

4. Меры защиты информации от угроз безопасности информации, реализуемых внутренними нарушителями

4.1. Отключить удаленный доступ к критичным системам и сетям, предоставляя его только по согласованной заявке и на короткий интервал времени для выполнения работ.

4.2. Реализовать запись действий привилегированного пользователя, включая RDP сессии (при возможности).

4.3. Организовать ролевую модель доступа пользователей таким образом, чтобы тот, кто имеет административный доступ к системам, не имел прав на удаление и модификацию резервных копий баз данных.

4.4. Внести изменения в процедуру проведения обновлений программного обеспечения. В особый период должны проводиться только критические обновления, прошедшие тщательную проверку безопасности.

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

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

5.2. 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.

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

5.4. 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).

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

5.6. 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).

6. Меры защиты информации систем и сетей организации при работе с электронной почтой в органе, организации

6.1. Рассмотреть возможность перехода на отечественные решения или сервисы по защите электронной почты.

6.2. Если организация не взаимодействует с иностранными контрагентами, запретить коммуникации на сетевом уровне по протоколу SMTP с зарубежными IP-адресами (при возможности).

6.3. Активировать механизмы проверки подлинности домена-отправителя с использованием технологий SPF, DKIM, DMARC (при возможности).

6.4. Настроить функции уведомления пользователей в тексте сообщения при получении от внешнего отправителя (при возможности).

6.5. Запретить использование почтового сервера в качестве открытого relay.

6.6. Создать отдельный электронный почтовый адрес, на который пользователи будут присылать подозрительные письма и проинформировать их об этом.

6.7. Использовать почтовую «песочницу».

6.8. Заблокировать получение пользователями систем и сетей электронных писем, имеющих вложения с расширениями ADE, ADP, .APK, APPX, APPXBUNDLE, BAT, CAB, CHM, CMD, COM, CPL, DLL, DMG, EX, EX_, EXE, HTA, INS, ISP, ISO, JAR, JS, JSE, LIB,

LNK, MDE, MSC, MSI, MSIX, MSIXBUNDLE, MSP, MST, NSH, PIF, PS1, SCR, SCT, SHB, SYS, VB, VBE, VBS, VHD, VXD, WSC, WSF, WSH.

7. Общесистемные меры защиты информации, а также систем и сетей

7.1. Обеспечить резервное копирование в изолированном сегменте системы. Провести тестирование восстановления из резервных копий. Доступ к этому сегменту должен быть минимизирован по белым спискам с запретом доступа из сети «Интернет».

7.2. Рассмотреть отечественные альтернативы зарубежным поставщикам информации об индикаторах компрометации (IoC).

7.3. Запретить отправку событий безопасности во внешние иностранные сервисы (Cloud SIEM, Cloud EDR, SOC и MDR).

7.4. Не использовать репозиторий хранения кода github для работы над собственными проектами. При необходимости развернуть свой изолированный сервер репозиториев.

7.5. Исключить применение сервисов обмена текстом, таких как Pastebin и его аналогов для передачи чувствительной информации, например, конфигурационных файлов, исходного программного кода. При необходимости развернуть частный сервис обмена текстом (например, privatebin).

7.6. Для оказания методической помощи по реализации приведенных в настоящем документе мер защиты информации специалисты по информационной безопасности могут обратиться в Управление ФСТЭК России по Северо-Западному федеральному округу по телефону 8 (812) 312-51-35 и в центральный аппарат ФСТЭК России (для федеральных систем и сетей) по телефонам 8(499)263-27-65 и 8(499)263-27-75.

7.7. В случае выявления признаков компьютерных инцидентов в системах и сетях необходимо незамедлительно проинформировать о них Национальный координационный центр по компьютерным инцидентам (тел.: 8 (916) 901-07-42; эл. почта: info@cert.gov.ru).