|  |  |
| --- | --- |
| **ФСТЭК РОССИИ**  **УПРАВЛЕНИЕ**  **ФЕДЕРАЛЬНОЙ СЛУЖБЫ**  **ПО ТЕХНИЧЕСКОМУ И**  **ЭКСПОРТНОМУ КОНТРОЛЮ**  **ПО ДАЛЬНЕВОСТОЧНОМУ**  **ФЕДЕРАЛЬНОМУ ОКРУГУ**  Ул. Ленина, д. 37, г. Хабаровск, 680030  Тел., факс (4212) 35-11-08  E-mail: dfo@fstec.ru  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2025 г. № \_\_\_\_\_\_\_\_\_\_\_  На № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Председателям Советов по информационной безопасности при главах высших исполнительных органов государственной власти субъектов Российской Федерации в Дальневосточном федеральном округе |

О мерах по повышению защищенности информационной инфраструктуры

По результатам анализа сведений об угрозах безопасности информации  
и деятельности хакерских группировок, проводимого специалистами ФСТЭК России  
в условиях сложившейся обстановки, выявлены сведения о деятельности хакерских группировок и распространяемом ими вредоносном программном обеспечении.

В соответствии с подпунктом «е» пункта 1 Указа Президента  
Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах  
по обеспечению информационной безопасности Российской Федерации» направляем организационные и технические меры по повышению защищенности информационной инфраструктуры органа (организации), подлежащие реализации.

1. Хакерской группировкой Paper Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем  
от лица ФСТЭК России. Во вложениях указанных писем прикреплен файл, замаскированный под легитимный документ. После запуска пользователем указанного файла осуществляется демонстрация письма ФСТЭК России, выполнение команд оболочки сценариев PowerShell и внедрение на целевую систему вредоносного программного обеспечения типа «загрузчик».

Для предотвращения реализации угроз безопасности информации, связанных  
с деятельностью указанной хакерской группировки по фишинговым рассылкам, необходимо принять следующие меры защиты.

1.1. Производить проверку почтовых вложений с использованием средств антивирусной защиты:

для антивирусного средства Kaspersky Endpoint Security необходимо использовать функцию «Защита от почтовых угроз». Для того чтобы включить указанную функцию, необходимо перейти в настройки приложения и в разделе «Базовая защита» активировать функцию «Защита от почтовых угроз»;

для антивирусного средства Dr.Web Security Space необходимо использовать утилиту SpIDer Mail. Для того чтобы задействовать указанную утилиту, необходимо перейти в настройки приложения и в разделе «Компоненты защиты» выбрать  
и активировать утилиту SpIDer Mail.

1.2. Проверять имя домена отправителя электронного письма в целях идентификации отправителя. Для этого необходимо обращать внимание  
на наименование почтового адреса (домена), указанного после символа «@»,  
и сопоставлять его с адресами (доменами) органов (организаций), с которыми осуществляется служебная переписка.

1.3. Организовать получение почтовых вложений только от известных отправителей. Для этого необходимо организовать ведение списков адресов электронной почты органов (организаций), с которыми осуществляется взаимодействие.

1.4. Не открывать и не загружать почтовые вложения писем с тематикой,  
не относящейся к деятельности органа (организации).

1.5. Осуществлять работу с электронной почтой под учетными записями пользователей операционной системы с минимальными возможными привилегиями:

для операционных систем семейства Microsoft Windows ограничение привилегий можно осуществить через «Панель управления» - «Учетные записи пользователей» - «Управление учетными записями»;

для операционных систем семейства Linux возможно использование команд chmod, chown, chgrp для разграничения прав доступа к файлам и директориям  
как отдельных пользователей, так и групп пользователей.

1.6 Ограничить возможность получения электронной почты с адреса postin@fstek[.]ru Обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

barrelize[.]org;

tributetropic[.]org;

hxxps[:]//barrelize[.]org/playhouse/dustbins/folkish/generators/curling;

hxxps[:]//tributetropic[.]org/playhouse/dustbins/folkish/generators/curlings[.]dotm.

Обращаем внимание, что редактирование в активное состояние ссылок  
на вредоносное программное обеспечение и серверы управления злоумышленников, приведенных в настоящем письме, а также переход по данным ссылкам не допускается, так как создает предпосылки к распространению вредоносного программного обеспечения.

1.7. Осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):

2318600c7bd150e8bf06b0301635598cc799ce2a9a60308027eb63a033f97ceb;

9641870ec560c0463d86f482cbd1cb6ea34c3db23d40ad80833cd59739cd33b6;

faf35266966ce5432b312d4120cafd95f1c6187db0f1f4b6d6c579c339d66f55;

19a848d4121b74b59438c3e0552e5f697180e1e2695f3e6adb353aed4915ca99;

1dcbf2774f505b45368ff0541da4117dce0e4763b85d9ccba20e7298b2425ec9;

580839bf75b910a2251f21f1cea006c6f1e84fcde03b696a7e8b163278042b80;

42c0e046e039029633683df8e192e6a0cb1621d387337d91e05339db8cffb94f;

677e4f461dca20c6e24efbefd47b115722b2eafbd2dc00718c08a393e687bd80;

ed41a4b1f989839a5ad97aaff30dbdf28aeb4fde6d3068a96cb83da27d298d5da.

2. Хакерской группировкой BO Team (Lifting Zmiy, Hoody Hyena), нацеленной  
на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых прикреплен файл с расширением «.pdf». После запуска пользователем указанного файла осуществляется внедрение на целевую систему вредоносного программного обеспечения типов «бэкдор» (DarkGate, BrockenDoor и Remcos) и «шифровальщик» (Babuk).

Для предотвращения реализации угроз безопасности информации, связанных  
с деятельностью указанной хакерской группировки по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.5.

Кроме того, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

invuln[.]xyz;

railradman[.]site;

dzeninfra[.]site;

dzeninfra[.]xyz;

sso[.]dzeninfra[.]site;

sso[.]dzeninfra[.]xyz;

wincertfm[.]store;

wmiadap[.]xyz;

wmiadap[.]sbs;

wmiadap[.]cfd;

194[.]190[.]152[.]251;

194[.]113[.]106[.]51;

193[.]124[.]33[.]172;

45[.]144[.]30[.]144;

193[.]124[.]33[.]184;

194[.]190[.]152[.]149;

194[.]87[.]252[.]221;

194[.]87[.]252[.]171.

Кроме того, необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий индикаторов компрометации, указанных в приложении  
к настоящим рекомендациям.

3. Хакерской группировкой PhantomCore, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры  
Российской Федерации, осуществляются фишинговые рассылки электронных писем  
с тематикой «Документы на рассмотрение (повторно)». Во вложениях указанных писем прикреплен архив с наименованием «Документы\_на\_рассмотрение.zip», внутри которого содержатся файл-приманка с наименованием «Сопроводительное\_письмо.pdf» и файл-ярлык с наименованием «Договор\_23702\_05\_05\_2025.pdf.lnk». После запуска пользователем указанного файла-ярлыка осуществляется демонстрация документа-приманки и внедрение на целевую систему вредоносного программного обеспечения типа «бэкдор» (PhantomeCore.GreqBackdoor v.2).

Для предотвращения реализации угроз безопасности информации, связанных  
с деятельностью указанной хакерской группировки по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.5.

Кроме того, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

supportsecure[.]ru;

supportsecurity[.]ru;

updatesioa[.]ru;

updatecanonical[.]ru;

rawgithubcontent[.]ru;

syncpulse[.]ru;

airgrupdate[.]ru;

mastersync[.]ru;

updateapi[.]ru;

195[.]133[.]32[.]194;

195[.]58[.]54[.]39;

update54[.]ru;

officesync[.]ru;

hxxp[:]//195[.]58[.]54[.]39[:]80/command;

hxxp[:]//195[.]58[.]54[.]39[:]80/init;

hxxp[:]//195[.]58[.]54[.]39[:]80/check;

hxxp[:]//195[.]58[.]54[.]39[:]80/connect.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):

278f051832c4b2c95ba899d685478bd3430f74d21aea367377cc17788c3a5638;

656a47064ee26b49204412889e7f2ff4c98ebb8579e01cca84679ff31688e6ea;

31cc62a06720e0c20f03e0cb912bb92b20e5f339ae9c7280b235f63ac35eda9a;

9287fd8adc333469eabe655ccf13b78e1abb6e42c0cc6817ae66372fb126a683;

c34fb316e7b60cff25be9c86e5736b802b9e99b1ac29daa03b08c3435b6ada8c;

c67cf425d688bba6dbe00e6d86a501f6978664ff99c1811c7104f4a3f4b7e884.

4. Хакерской группировкой Vengeful Wolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем  
с тематикой «Акт сверки». Во вложениях указанных писем прикреплен архив  
с наименованием «1.zip». Архив содержит файл-приманку с наименованием «Образец.rtf» и исполняемый файл с наименованием «Aкт cвepки взaимopacчeтoв  
пo cocтoянию нa 28.05.2025 гoдa.scr». После запуска пользователем указанного исполняемого файла осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа» (Revenge RAT).

Для предотвращения реализации угроз безопасности информации, связанных  
с деятельностью указанной хакерской группировки по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.5.

Кроме того, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к адресам, указанным в приложении к настоящим рекомендациям, используя схему доступа по «черным» или «белым» спискам.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий индикаторов компрометации, указанных в приложении к настоящим рекомендациям.

5. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых прикреплен исполняемый файл с расширением «.msi». После запуска пользователем указанного исполняемого файла осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «троян удаленного доступа».

Для предотвращения реализации угроз безопасности информации, связанных  
с деятельностью указанных хакерских группировок по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.5.

Кроме того, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

18[.]231[.]162[.]77;

107[.]174[.]231[.]26;

142[.]54[.]185[.]178;

54[.]207[.]88[.]51;

atual2025[.]com;

clientepj[.]com;

computadorpj[.]com;

financial-executive[.]com;

hamrah-tejarat[.]com;

nfe-fiscal[.]com;

ranchocentral[.]com;

servidor2025[.]com;

syarousi-search[.]com;

nf-eletronica[.]org;

relay[.]lombrelone[.]com;

webrelayapi[.]online;

hxxps[:]//github[.]com/contaaws20251.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий индикаторов компрометации, указанных в приложении  
к настоящим рекомендациям.

6. Хакерской группировкой Cloud Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых прикреплен файл с наименованием «О восстановлении документов гражданину Беларуси.doc». После запуска пользователем указанного файла осуществляется выполнение вредоносного VBS-скрипта и внедрение на целевую систему вредоносного программного обеспечения типа «бэкдор» (VBShower, VBCloud и PowerShower).

Для предотвращения реализации угроз безопасности информации, связанных  
с деятельностью указанной хакерской группировки по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.5.

Кроме того, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к адресу hxxps[:]//transferpolicy[.]org/?plugins\_cherry-team-members/public/assets/css/font-awesome[.]min[.]css/preobviously, используя схему доступа по «черным» или «белым» спискам.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующего индикатора компрометации (sha256):

5e9b2f0121695f55d7de6a6e3385a68cab37cce8982de2ccd541e698e249166c.

7. Хакерской группировкой Stone Wolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры  
Российской Федерации, осуществляются фишинговые рассылки электронных писем,  
в тексте которых прикреплена ссылка на загрузку архива, содержащего исполняемый файл, замаскированный под легитимный PDF-документ. После запуска пользователем указанного файла осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «бэкдор» (BrockenDoor).

Для предотвращения реализации угроз безопасности информации, связанных  
с деятельностью указанной хакерской группировки по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.5.

Кроме того, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

rzd-partner[.]pro;

rzd-partner[.]store;

194[.]190[.]153[.]198;

hxxps[:]//rzd-partner[.]store/RZD\_Forum\_28[.]05[.]rar;

hxxps[:]//rzd-partner[.]pro/RZD\_Forum\_28[.]05[.]rar;

hxxp[:]//194[.]190[.]153[.]198[:]7194/t.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):

322d51d71780f700cfb3917741b4567f6ab88d8b854229c9bffab6f2ac6b2338;

6d69e302fcce1cf680e696e75de2623a2384b9871ec75ef13e9c2bc7c98f701a;

429b0362eeeebb0886f09beda98196c8247f2e2db50822ff62de773ef1fe8b0b;

63fb3d9e3d5820997a24ad240c617099bc27fe9b61247b8134cf6b6ffaac3527;

091bd6efb4cb2cdc546fb109079ac9214f3d6b6448cf3dcda3c7a31f1b2e30da;

7cb5488440f9ad666c4ae1aa50fae09ba9742514d52e3b2f4bac6ffb2e350091;

0b5fe6633ac65ae28a444d6d91532e0c605c184ebd3d7945b07a871b42aeec37;

b820d1c3bb8ae60efca9f08836fce4e0b3e5407c83a1f6af82c55c911603cb99;

3baa3844839a73155545d31d2d5761b5c283746d1bbe828bef3a83bd2cb4372e;

1a3ea28f0c15beed5bdc051b3525db390927212dfd76ba8e4e89afa0d2577a3e.

8. Хакерской группировкой Sapphire Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем,  
в тексте которых прикреплена ссылка на загрузку архива, содержащего исполняемый файл с наименованием «Служебная записка.exe», замаскированный под легитимный PDF-документ. После запуска пользователем указанного файла осуществляется внедрение на целевую систему вредоносного программного обеспечения типа «стилер» (AmethystStealer).

Для предотвращения реализации угроз безопасности информации, связанных  
с деятельностью указанной хакерской группировки по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.5.

Кроме того, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

hxxp[:]//elk-divine-immensely[.]ngrok-free[.]app/;

hxxps[:]//elk-divine-immensely[.]ngrok-free[.]app/;

hxxp[:]//canarytokens[.]com/traffic/tags/static/xjemqlqirwqru9pkrh3j4ztmf/payments[.]js.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):

e30a77f93998b2cd96eb48195df53c9bf3e8b53d1fdf827b5a577fe149f0290f;

23b2fe3498f136f5a7f2e3dbbd0560116f1fc82b7f635349ab0c08fbaca4e9bf;

afebef5c1029dc102a8a18fda2bf93d9ee2af3d29d80479a3c22ee18d6f169bf;

95258dfa06e459d91672b707a743a423a1d00484ba26e0426fb6715c12f6b2de;

9eb1254e6343e0184e0a81972e0860dba0da24fea387a0c05c0c8660442a69c1.

9. Хакерской группировкой PhaseShifters, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры  
Российской Федерации, осуществляются фишинговые рассылки электронных писем от лица Министерства образования и науки Российской Федерации. Во вложениях указанных писем прикреплен архив с наименованием «Исходящий от 26.05.2025.7z», содержащий файл-приманку с наименованием «Prilozenie\_k\_pis\_mu.docx»  
и исполняемый файл с наименованием «Pis\_mo\_zapros\_na\_predpriatia\_OPK.doc.exe.exe», после запуска пользователем которого осуществляется демонстрация документа-приманки и внедрение вредоносного программного обеспечения типа «троян удаленного доступа» (QuasarRAT).

Для предотвращения реализации угроз безопасности информации, связанных  
с деятельностью указанной хакерской группировки по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.5.

Кроме того, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

193[.]124[.]33[.]207;

minobnauki[.]ru;

5[.]8[.]11[.]119;

min-prom[.]ru;

mail[.]min-prom[.]ru;

superjoke[.]ru;

forum-drom[.]ru;

cloud-telegram[.]ru;

about-sport[.]ru.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (md5):

2b7004cb00d58967c7d6677495d3422e;

0bbb3a2ac9ba7d14a784cbc2519fbd64;

40ef2615afb15f61072d7cea9b1a856a;

681af8a70203832f9b8de10a8d51860a.

10. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лица федерального казенного предприятия «ГЛП «РАДУГА» с тематикой «СРОЧНО: необходима ваша реакция по вложенному документу». Во вложениях указанных писем прикреплен файл с наименованием «Акт\_внутренней\_проверки\_контрагента\_срочно.pdf (10).pdf».  
При открытии указанного файла пользователю предлагается выполнить ряд команд  
для ознакомления с содержимым документа, после чего осуществляется внедрение  
на целевую систему вредоносного программного обеспечения типа «дроппер».

Для предотвращения реализации угроз безопасности информации, связанных  
с деятельностью указанных хакерских группировок по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.5.

Кроме того, необходимо обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

77[.]110[.]104[.]115;

docrf[.]org;

hxxps[:]//docrf.org/rjPiWMqwPx0PQE931FDXo9fNcMH1SB7c/.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующего индикатора компрометации (sha256):

e7b58b7fee52dd577219cc5c5d6926fb63c4e5f71aaed932e62ae623a698926d.

11. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем с тематикой «Схема оповещения!». Во вложениях указанных писем прикреплен запароленный архив  
с наименованием «1. СХЕМА ОПОВЕЩЕНИЯ РЕЖИМ КОВЕР.docx.rar», внутри которого содержится исполняемый файл с наименованием «1. СХЕМА ОПОВЕЩЕНИЯ РЕЖИМ КОВЕР.docx.scr». После запуска пользователем указанного файла осуществляется демонстрация документа-приманки, выполнение команд оболочки сценариев PowerShell и внедрение на целевую систему вредоносного программного обеспечения типа «загрузчик».

Для предотвращения реализации угроз безопасности информации, связанных  
с деятельностью указанных хакерских группировок по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.5.

Кроме того, необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):

265f04de875ab37b33d1d7716a28768785fb40f44b159c6276b015c4d4cb73c3;

315691c6682b8623b021d6421ebe64fc6469aae179c33987cf0b771ac3904cf5;

01793e6f0d5241b33f07a3f9ad34e40e056a514c5d23e14dc491cee60076dc5a;

eda75a90bcd551c724b8a8d0bf2b5e69c430088dc249fe9e79d8509b57d96a30;

e8a432e612369f9180ec907966a24c2d8924e29fd1b70c618368e4dbc19557a9;

d98465c6710f4326b3f30fb4c791560a78243175c93d146b84e6fc2d0a965795;

cca5879951cc62bb23f3ad8b72e8e74bc4888e0c8c1941dc30304480d865eecb;

727df710433850e751c1ae0b10cabf7d332d8072b4fa6501bc2ff3a0429c9f18.

12. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, возможно применение при осуществлении целевых компьютерных атак вредоносного программного обеспечения типа «бэкдор», предназначенного для обхода настроек аутентификации Linux Pluggable Authentication Modules (PAM), в целях получения доступа к целевой системе.

Для предотвращения реализации угроз безопасности информации, связанных  
с деятельностью указанных хакерских группировок, необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):

f62624d28aaa0de93e49fcdaaa3b73623723bdfb308e95dcbeab583bdfe3ac64;

24d71c0524467db1b83e661abc2b80d582f62fa0ead38fdf4974a64d59423ff1;

5aeae90e3ab3418ef001cce2cddeaaaea5e4e27efdad4c6fa7459105ef6d55fa;

ae26a4bc9323b7ae9d135ef3606339ee681a443ef45184c2553aa1468ba2e04b;

ac32ed04c0a81eb2a84f3737affe73f5101970cc3f07e5a2e34b239ab0918edd.

О результатах выполнения указанных рекомендаций прошу проинформировать Управление ФСТЭК России по Дальневосточному федеральному округу по адресу электронной почты dfo\_otd9@fstec.ru до 5 июля 2025 г. в форме письма с электронным вложением в формате PDF.

Приложение: Файловые индикаторы компрометации на 6 л.

|  |  |
| --- | --- |
| Руководитель Управления | В.Цалко |

Исп. и отп. Комарова Т.А.

тел. (4212) 35-11-75

09.06.2025