Бюллетень информационной безопасности от 19.02.2025

I. Сведения об уязвимостях.

Обращаем внимание на зафиксированные специалистами ФСТЭК России уязвимости, отнесенные к категории «наиболее опасные уязвимости».

1. Уязвимость сервиса для управления бизнесом Битрикс24 и **системы управления содержимым сайтов (CMS) 1С-Битрикс: Управление сайтом** (BDU:2025-00765, уровень опасности по CVSS 3.0 – высокий), связанная с непринятием мер по защите структуры веб-страницы. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код путем отправки специально сформированного HTTP-запроса.

В целях предотвращения возможности эксплуатации данной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования обновлений безопасности программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г. (далее – «Методика тестирования»), а также Методикой оценки уровня критичности уязвимостей программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г. (далее – «Методика оценки») (https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty).

В случае невозможности установки обновления программного обеспечения рекомендуется принять следующие компенсирующие меры:

использовать межсетевой экран уровня приложений;

использовать «белый» список IP-адресов для ограничения доступа к веб-интерфейсу управления программным средством;

использовать средства обнаружения и предотвращения вторжений для отслеживания попыток эксплуатации уязвимости;

использовать виртуальные частные сети для организации удаленного доступа.

2. Уязвимость функций ss_net_snmp_disk_io() и ss_net_snmp_disk_bytes() программного средства мониторинга сети Cacti (BDU:2025-00856, уровень опасности по CVSS 3.0 – критический), связанная с непринятием мер по нейтрализации специальных элементов, используемых в команде операционной системы. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код путем отправки специально сформированных SNMP-запросов, содержащих некорректные OID-идентификаторы.

В целях предотвращения возможности эксплуатации данной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования и Методикой оценки ФСТЭК России.

В случае невозможности установки обновления программного обеспечения рекомендуется принять следующие компенсирующие меры:

использовать средства межсетевого экранирования с поддержкой технологии глубокой проверки сетевых пакетов для фильтрации вредоносных SNMP-пакетов;

использовать «белый» список IP-адресов для ограничения доступа к веб-интерфейсу управления уязвимым программным обеспечением;

использовать средства обнаружения и предотвращения вторжений для отслеживания попыток эксплуатации уязвимости.

3. Уязвимость функции ksmbd_vfs_stream_read() демона KSMBD ядра операционной системы Linux (BDU:2025-00883, уровень опасности по CVSS 3.0 – критический), связанная с выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, раскрыть защищаемую информацию и вызвать отказ в обслуживании путем отправки специально сформированных SMB-запросов к файлам с ADS.

В целях предотвращения возможности эксплуатации данной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования и Методикой оценки ФСТЭК России.

В случае невозможности установки обновления программного обеспечения рекомендуется принять следующие компенсирующие меры:

разрешить подключение к SMB-серверу только доверенным пользователям;

использовать средства обнаружения и предотвращения вторжений для отслеживания попыток эксплуатации уязвимости;

использовать SIEM-системы для отслеживания событий журнала, связанных с получением SMB-запросов;

использовать виртуальные частные сети для организации удаленного доступа;

ограничить доступ к устройствам из внешних сетей.

4. Уязвимость функции nft_setelem_catchall_deactivate() в модуле net/netfilter/nf_tables_api.c ядра операционной системы Linux (BDU:2024-01186, уровень опасности по CVSS 3.0 – высокий), связанная с повторным использованием ранее освобожденной памяти. Эксплуатация уязвимости может позволить нарушителю оказать воздействие на конфиденциальность, целостность, доступность защищаемой информации и повысить свои привилегии.

5. Уязвимость функции nft_set_rbtree (net/netfilter/nft_set_rbtree.c) компонента Netfilter операционной системы Linux (BDU:2024-01724, уровень опасности по CVSS 3.0 – высокий), связанная с выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

6. Уязвимость функции nf_tables_abort() в модуле net/netfilter/nf_tables_api.c компоненты netfilter ядра операционной системы Linux (BDU:2024-04369, уровень опасности по CVSS 3.0 – высокий), связанная с некорректной блокировкой ресурса. Эксплуатация уязвимости может

позволить нарушителю оказать воздействие на конфиденциальность, целостность и доступность защищаемой информации.

7. Уязвимость компонента nf_tables netfilter ядра операционной системы Linux (BDU:2025-00432, уровень опасности по CVSS 3.0 – высокий), связанная с использованием памяти после ее освобождения. Эксплуатация уязвимости может позволить нарушителю вызвать отказ в обслуживании или повысить свои привилегии путем отправки специально созданного запроса.

8. Уязвимость компонента ipset ядра операционной системы Linux (BDU:2024-10986, уровень опасности по CVSS 3.0 – высокий), связанная с использованием памяти после ее освобождения. Эксплуатация уязвимости может позволить нарушителю повысить привилегии в системе.

В целях предотвращения возможности эксплуатации указанных в пунктах 4-8 уязвимостей рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования и Методикой оценки ФСТЭК России.

9. Уязвимость драйвера вспомогательных функций (реализации) прикладного программного интерфейса Winsock операционных систем Windows (BDU:2025-01475, уровень опасности по CVSS 3.0 – средний), связанная с переполнением буфера в динамической памяти. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии до уровня SYSTEM путем отправки специально сформированных запросов.

В целях предотвращения возможности эксплуатации данной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования и Методикой оценки ФСТЭК России.

В случае невозможности установки обновления программного обеспечения рекомендуется принять следующие компенсирующие меры:

использовать SIEM-системы для отслеживания попыток эксплуатации уязвимости;

использовать системы обнаружения и предотвращения вторжений для отслеживания индикаторов компрометации;

произвести минимизацию пользовательских привилегий;

отключить (удалить) неиспользуемые учетные записи пользователей.

10. Уязвимость функции nft_set_commit_update() в модуле net/netfilter/nf_tables_api.c компонента netfilter ядра операционной системы Linux (BDU:2024-00096, уровень опасности по CVSS 3.0 – средний), связанная с повторным использованием ранее освобожденной памяти. Эксплуатация уязвимости может позволить нарушителю с полномочиями CAP_NET_ADMIN оказать воздействие на конфиденциальность, целостность и доступность защищаемой информации и повысить свои привилегии.

В целях предотвращения возможности эксплуатации данной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования и Методикой оценки ФСТЭК России.

В случае невозможности установки обновления программного обеспечения рекомендуется запретить пользователям с полномочиями CAP_NET_ADMIN удалять наборы (set) netfilter.

11. Уязвимость функции queue_oob() в модуле net/unix/af_unix.c реализации сокетов AF_UNIX ядра операционной системы Linux (BDU:2024-04563, уровень опасности по CVSS 3.0 – средний), связанная с повторным использованием ранее освобожденной памяти из-за конкурентного доступа к ресурсу (состояние гонки). Эксплуатация уязвимости может позволить нарушителю вызвать отказ в обслуживании.

12. Уязвимость компонента Netfilter ядра операционной системы Linux (BDU:2025-00024, уровень опасности по CVSS 3.0 – средний), связанная с неправильным контролем идентификаторов ресурсов. Эксплуатация уязвимости позволяет нарушителю повысить свои привилегии.

13. Уязвимость функции bpf_ringbuf_reserve() ядра операционной системы Linux (BDU:2025-00022, уровень опасности по CVSS 3.0 – средний), связанная с выделением неограниченной памяти. Эксплуатация уязвимости может позволить нарушителю вызвать отказ в обслуживании.

14. Уязвимость компонента bpf ядра операционной системы Linux (BDU:2025-01090, уровень опасности по CVSS 3.0 – средний), связанная с использованием памяти после ее освобождения. Эксплуатация уязвимости может позволить нарушителю повысить привилегии в системе.

В целях предотвращения возможности эксплуатации указанных в пунктах 11-14 уязвимостей рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования и Методикой оценки ФСТЭК России.

II. Сведения о деятельности хакерских группировок.

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.

1. Хакерской группировкой Rare Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лица представителей ООО «Центр Экономико-правового анализа и сопровождения контрактов в промышленности «Контрактный Центр» и Минпромторга России. Во вложениях указанных писем содержится вредоносный исполняемый файл, после запуска пользователем которого осуществляется демонстрация документа-приманки, загрузка и внедрение легитимного программного обеспечения для удаленного доступа «AnyDesk».

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. Обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

vniir[.]space;

hxxp[:]//vniir[.]space/file/Trays[.]rar;

hxxp[:]//vniir[.]space/file/driver[.]exe;

hxxp[:]//vniir[.]space/file/pas[.]rar.

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):
e880a1bb0e7d422b78a54b35b3f53e348ab27425f1c561db120c0411da5c1ce9;
25212e1c8a3734c4a17f07cfcb4ff35d25d8de32efc564f471edfab3f120aa2b;
8b6afbf73a9b98eec01d8510815a044cd036743b64fef955385cbca80ae94f15;
28a75c16ba5774df65b5d01eb7f5067950cd5b9796c05baceeb85ac38d100d6b;
7d6b598eaf19ea8a571b4bd79fd6ff7928388b565d7814b809d2f7fdedc23a0a;
8bdb8df5677a11348f5787ece3c7c94824b83ab3f31f40e361e600576909b073;
c5eeec72b5e6d0e84ff91dfdcbefbbbf441878780f887febb0caf3cbe882ec72;
d8edd46220059541ff397f74bfd271336dda702c6b1869e8a081c71f595a9e68;
893e169b5902b7871d57ad73d88008e6a8a14a3c595180bcfdad19f306eef58b;
bb243113d236f823abd1839025190e763fe34c40da4949b77558995cc1a07625;
e0463b1e4b3505eb19b01b6488c21d07321fc613c6689cd89e699455917b4e9f;
89c80662c90deea257296848206af7c0eaf58ba9f9f097d5d8ec91826047f567.

2. Хакерской группировкой Watch Wolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится вредоносный исполняемый файл с наименованием «Заявка январь 2025.exe». После запуска пользователем указанного исполняемого файла осуществляется выполнение JS-скриптов и внедрение вредоносного программного обеспечения типа «бэкдор» (DarkWatchman).

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:

fb0bf2b1[.]site;

fb0bf2b1[.]online.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
bb8eeeb4e2519b8b34448b7be063f3b8ab058af691df24eebac5d8db9259de91;
16ba582d17b3481152909d12ed2098196887697481bc2afb32d41d044e2bf58d;
d0fc980288bcba28b18d99c345dafe4d407099edbe4819e9ace0de39b13f3d5a.

3. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лица горнодобывающей компании Азербайджана с тематикой «Заявка». Во вложениях указанных писем

содержится архив с наименованием «DF033883892.zip», внутри которого находится вредоносный исполняемый файл с наименованием «okCz6M2stQwRX4M.exe». После запуска пользователем указанного исполняемого файла осуществляется внедрение 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, а также заблокировать получение электронных писем с адреса aykhan[.]eyvazov@starmining[.]az.

Кроме того, необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
a4160cf550242c05db20165f66a451d9698b391785c7798e366544804b713575;
afd88fd9cf58f5b47a3d0410149695bd2fc4eda189cd1216b07a76a4469c4a7b.

4. Хакерской группировкой Hellhounds, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится вредоносный файл с наименованием «33». После запуска пользователем указанного файла осуществляется загрузка и внедрение вредоносного программного обеспечения «троян удаленного доступа» (DecoyDog и PupyRAT).

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:

185[.]143[.]221[.]125;
194[.]87[.]68[.]65;
5[.]252[.]176[.]45;
5[.]252[.]176[.]63;
52[.]184[.]34[.]71;
91[.]210[.]107[.]141.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
03b007a5fbb9d1556b4bedd6e930463ce35f5ae17b245edc58c12eb086de891f;
d189e0150f42d2a2e40fefcec6973fcbc4a8b1a1757a358d13df3519ef275412.

5. Хакерскими группировками HellCat и Morpheus, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится вредоносный файл с наименованием «100M*.exe». После запуска пользователем указанного файла осуществляется загрузка и внедрение вредоносного программного обеспечения типа «шифровальщик».

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:

hellcakbszllztlyqbjzwcbdhfrodx55wq77kmftp4bhnhsnn5r3odad[.]onion;

izsp6ipui4ctgxfugbgtu65kzefrucltyfpbxplmfybl5swiadpljmyd[.]onion;

hellcat[.]locker.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha1):

b834d9dbe2aed69e0b1545890f0be6f89b2a53c7;

f62d2038d00cb44c7cbd979355a9d060c10c9051;

f86324f889d078c00c2d071d6035072a0abb1f73.

6. Хакерской группировкой Bloody Wolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, в которых говорится о нарушении органом (организацией) налогового законодательства. Во вложениях указанных писем содержится документ с расширением «.pdf», в тексте которого пользователю предлагается скачать дополнительные документы, перейдя по ссылкам. После перехода по указанным ссылкам осуществляется загрузка вредоносного файла с расширением «.jar». После запуска пользователем указанного файла осуществляется внедрение легитимного программного обеспечения для удаленного доступа «NetSupport».

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 настоящему письму, 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 настоящему письму.

7. Хакерской группировкой Squid Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится вредоносный файл с наименованием «StatRKZU.msi». После запуска пользователем указанного файла на целевую систему осуществляется установка легитимного программного обеспечения «Статистика КЗУ», а также выполнение Batch-скрипта для внедрения вредоносного программного обеспечения типа «троян удаленного доступа» (Konni).

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью хакерских группировок по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.5. Обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

88zr7cua[.]atwebpages[.]com;
5s6bqbea[.]sportsontheweb[.]net;
g66nzt8q[.]mygamesonline[.]org;
p593d8g9[.]mygamesonline[.]org;
tl2j38w9[.]mypressonline[.]com;
3cym4ims[.]medianewsonline[.]com;
c6cdg4su[.]sportsontheweb[.]net;
99695njd[.]myartsonline[.]com;
w9uzs9la[.]mywebcommunity[.]org;
cor8xcib[.]getenjoyment[.]net;
t8nptw2h[.]mywebcommunity[.]org;
zomfaa9a[.]onlinewebshop[.]net;
24ev0apa[.]scienceontheweb[.]net;
j1p75639[.]medianewsonline[.]com;
694qf6w8[.]scienceontheweb[.]net;
victory-2024[.]mywebcommunity[.]org;
p8tebfel[.]getenjoyment[.]net;
jbkza9h7[.]atwebpages[.]com;
mhhnv7s9[.]myartsonline[.]com;
zcvbm1zv[.]onlinewebshop[.]net;
mbfasq54[.]mypressonline[.]com.

Осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
b792867d9275c0ed64cbb501431fe0368c08ee3fa284a72590e46881241b2076;

b60dc12833110098f5eec9a51749d227db7a12d4e91a100a4fd8815695f1093f;
58bcd90f6f04c005c892267a3dfe91d1154d064482b07715ad5802f57c1ea32d;
9339eaf1d77bb0324e393a08a6180fe0658761fc0cd20ba25081963286dfb9c7;
a56a8217bad8523c3f2f163a69a50fba79142ab0a71b4a1443fb4143847e7146.

8. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, в тексте которых пользователю предоставляется ссылка на сайт для ознакомления с зарплатной ведомостью с наименованием «2025_SALARY_SLIP». После перехода пользователем по указанной ссылке предлагается авторизоваться в указанном сервисе для ознакомления с документом-приманкой. Таким образом злоумышленники осуществляют сбор аутентификационных данных.

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, а также заблокировать получение электронной почты с адреса MAILER-DAEMON@vps[.]floralands[.]com.

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

hxxps[:]//emailbrigade[.]pages[.]dev/abelhd?login=n_sadchikov@rn-bunker[.]rosneft[.]ru&

emailcomms[.]trapoli[.]top;

emailer[.]derart[.]click;

cypherloop[.]online.

9. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лица ООО «5.25 Программы». Во вложениях указанных писем содержится файл с наименованием «Swift 223445-1-1-1-1 (1).pdf», после запуска пользователем которого осуществляется демонстрация документа-приманки. Указанный документ предлагает пользователю осуществить регистрацию для ознакомления с полной версией документа. Таким образом злоумышленники осуществляют сбор аутентификационных данных.

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 адресу hxxps[:]//rigorous-nutritious-parsley[.]glitch[.]me, 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 следующих индикаторов компрометации (sha256):

828c720538b83e4a519ffd6ba0587cda5084c9a6adfdecb079ca68eda9e631c2;

f3594c65a06f91da43aa9fe9e7b9adc92146557673be5b793bc23082c0f35e80.

10. Хакерской группировкой Cloud Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержатся вредоносные файлы с наименованиями «Типовая форма отзыва об исполнении научным работником должностных обязанностей.rtf» и «Образец биографической справки.rtf». После запуска пользователем указанных файлов осуществляется внедрение вредоносного программного обеспечения типа «бэкдор» (VBShower), путем эксплуатации уязвимости редактора математических формул и уравнений текстового редактора Microsoft Word, пакета программ Microsoft Office и пакета обеспечения совместимости Microsoft Office Compatibility Pack, текстового редактора Microsoft Word (BDU:2018-00246, уровень опасности по CVSS 3.0 – высокий).

В целях предотвращения возможности эксплуатации данной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования и Методикой оценки ФСТЭК России.

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:

hxxps[:]//block-monitor[.]net/?stocks_indian-energy-exc-ltd-share-price/INE022Q01020/idiogastrav;

hxxps[:]//block-monitor[.]net/?panel_knowledgebase/bladygrass.

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

81ab65c7b54f501a2e2962346764a6dcb587f32d5ee62b3569a4ba348152fdb9;
9ca81de013b9f9de63c80275fb662510241f97c4d1daab10ab6418a9d0a89cb6;
26295b543d1cb6cce1337cc06c1c8a8a0ee30e9aac580710f26bff7d5cc18193;
92088064194a9960d43d70db1452978c7bd325436d798e5b5fe25289fe79d112;
fd8a336452c27fcb65b88e0d47e888e683d5bacb63c140926c4a0557b4b48d80;
97497246227ef159a1bedf6ce97c8b81eb9cc86d34f5fbd00d7fe31862b3946d;
25230923690d4ce004d0592eac057f8d4ceb942f8334fb9d28d1363271ad3c89;
a9f53fc9f350446632111b500550567a8273d0f7838d27099c41f523a0a550b9;

a8bf032dea0fec1c6ef2926edcc03baedcadae149fcbcfb75925a98f290408cf;
1031e6d27ac96e53a4a3f5d5072029fca47b8b9b703860b5ab61bb06be777075;
366f6984d8aa9e78bca46788162f510bbafc10ede3d3ad4c4f53fb42bee00c55;
b2769bc8a25ee6b65e58b6f2795316d67771c54b9a423bf02c3779d63b08bc4a;
55f3f668364b3986a2c4ea528d00031c7a0ab67df54cef8affe92a21737f86c9;
5928b83d2626a85231618d6ba169a0133530a71bb71104c948b4b30e45aef0e0;
69b3f4877c7e051dc87d78b8d760e34b6a60000a10ea64351b577d6cb4df8967;
9047d2116b226b35170d1e8a7c81ce0fd25822f6bdf21db39fa3fd28700420a8;
f482cfe98e589bffd7eee76be5caf4040c69d4c0a8efbd10dcffaefab146ecd4;
957bbadda00231d45959c3f900d6ac805afbb1cb086192ad68549f3cf0cb8ec2;
1aaf4c0e8653d11adf5d36096130bb3d76384e932a476ae104eefcc0f9823d72;
1c5df7daf20c2235e7576b7399d83a85acad8252b08d07135b2481118a7c47ce;
d9c670f4b5c67958c8f8d705d66c0dbc2ab95e8edc441903e0c68de0aa7b4379;
31978d00e77c3d043116563d1b23e44fecba5c01b0fd17c1a0d2f4811294800d;
aa509fe7b7d6531866c3506e2c006e31926504685e685d93f658e3efb709400e;
3d55f9a70a1b01432fc0432e5b43ff6c8fa4a8a7a9ed5a787d9cf2a579b12c80;
678b30bcb599663bc7c26b4dc2ba49ee34048841c83531ca7c7f5ea2e3dee962;
614e7290bf7974e22e7eac04c1443565ca52e626f9ce4f93f8f33468293c7556;
a5ad86dd7e6b35b45957e9b0986b5fc633a0968d2887b702e1753a469ec57407;
75b2e65bebea849d0bd0bab6599f477e6ebd0e74c2ffa960d2360db771e3f583;
7b0683a60a10657963cbcfcc9d0480e7812a3894ffb3b0d6d92bab0dc2fde0b4;
c4f97cd48cc2ca11acc9e49ac18b8763752853beaabf149fe313b295fa01b2d6;
2e73cde9ce49cfd1970824f23d1fd4afd9b139f18f1aafc523814ecbdf4550ee.

11. Хакерской группировкой Kimsuky, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержатся вредоносные файлы с расширениями «.lnk», замаскированные под файлы Microsoft Office. После запуска пользователем указанных файлов осуществляется выполнение команд оболочки сценариев «PowerShell», загрузка и внедрение вредоносного программного обеспечения типов «кейлоггер», «загрузчик» и «троян удаленного доступа».

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:

216[.]219[.]87[.]41;

74[.]50[.]94[.]175.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем

внесения в правила корреляции событий следующих индикаторов компрометации (md5):

04e5f813da28b5975d0b6445f687bc48;
26d96d40e4c8aed03d80740e1d5a4559;
2ea71ff410088bbe79f28e7588a6fb47;
3211ef223177310021e174c928f96bab;
5565b337bfba78970b73ae65b95f2c4f.

12. Хакерской группировкой Rare Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, в которых содержится архив с наименованием «Письмо в МНТЦ и ЦРП.rar». Внутри указанного архива содержится вредоносный файл с наименованием «Письмо в МНТЦ и ЦРП.scr», замаскированный под официальный документ. После запуска пользователем указанного файла осуществляется внедрение легитимного программного обеспечения для удаленного доступа «AnyDesk».

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, а также заблокировать получение электронной почты с адреса silaev1968@mail-cheker[.]nl.

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

mail-cheker[.]nl;
hxxp[:]//mail-cheker[.]nl/down/AnyDesk[.]exe;
hxxp[:]//mail-cheker[.]nl/down/Trays[.]rar;
hxxp[:]//mail-cheker[.]nl/down/driver[.]exe;
hxxp[:]//mail-cheker[.]nl/down/pas[.]rar;
hxxp[:]//mail-cheker[.]nl/down/bat[.]bat;
hxxp[:]//mail-cheker[.]nl/down/bat1[.]bat;
hxxp[:]//mail-cheker[.]nl/down/pas[.]rar;
hxxp[:]//mail-cheker[.]nl/down/ps[.]ps1;
hxxp[:]//mail-cheker[.]nl/down/task[.]bat.

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

8d059a77ff3f3b0e0dd2e7b7fc433eda9ebf2ca4675ac0f2e6178ab135d1828f;
480f91e7b421e7a4a912f403806c40712cb43f87ee5254062acabb657d736f30.

13. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лица ФСТЭК России с тематикой «О запросе

информации». Во вложениях указанных писем содержится вредоносный архив с наименованием «запрос5161.7z», внутри которого находится вредоносный файл с наименованием «20250203_5_161.scr». После запуска пользователем указанного файла осуществляется демонстрация документа-приманки, загрузка и внедрение вредоносного программного обеспечения типа «ботнет».

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 адресам, указанным в приложении, 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 следующих индикаторов компрометации (sha256):
a0488131f969c4f4873e24a7bbce6dabac5cb9ff80e04421140ed9f663695c98;
27967a3dcacf33a5698c419576864aa1fc5bf1a541a9d28ce15527f4e53d9bcf;
8c84b9675272ec471c3d9b1b10957bf9f8676f17a491b15099eaa9ff1625a75a;
f2406609b6424d1a9fb4e09b7e3be8c960e6e9c48e7203be0e226f3a658ea504;
f2760a8ae2c82006b14c93e2256a345b525b7caa96d50575e5e2e5f378a17abe;
edcee35dba8091b669c3c24b1c9305f764d9f3b0bcd3dc72684c49d685f1fc51;
ca668005aec1ba623f104144e7ebb9c74d8ca45fe0d9d5b4b1bcbf4cc14caa6e;
c6459fe53d53cbb720269a41b547b5009c09cf3097e2bce600fed14844fdc136.

14. Хакерской группировкой TA558 (Romantic Wolf), нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится вредоносный файл с расширением «.rtf». После открытия пользователем указанного файла осуществляется эксплуатация уязвимости пакета программ Microsoft Office, связанной с неправильной обработкой объектов в памяти (BDU:2018-00096, уровень опасности по CVSS 3.0 – высокий), которая позволяет злоумышленникам запустить HTA-файл со скрытым обфусцированным VBS-сценарием. После выполнения данного сценария в целевой системе осуществляется внедрение вредоносного программного обеспечения типа «троян удаленного доступа» (Remcos RAT).

В целях предотвращения возможности эксплуатации данной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования и Методикой оценки ФСТЭК России.

Для предотвращения реализации угроз безопасности информации, связанных с деятельностью хакерских группировок по фишинговым рассылкам, необходимо реализовать меры защиты, указанные в пунктах 1.1-1.5. Обеспечить на уровне сетевых средств защиты информации ограничение

обращений к указанным в приложении адресам, используя схему доступа по «черным» или «белым» спискам.

Осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
b831341b086efa1e78ad9ba8ace189cb6425a55391709c08846060fe2a0858f8;
2615077b99ff9d89ea583e4d1ec3b998c61362167f7f79fddda74db7b4e60948.

15. Хакерская группировка Misty Werewolf (DaggerFly) при осуществлении компьютерных атак применяет набор вредоносных программ (ELF/Sshdinjector.A!tr), которые внедряют вредоносные библиотеки и двоичные файлы в службу SSH в целях компрометации целевой системы. Внедрение вредоносного программного обеспечения начинается с того, что «дроппер» проверяет, заражена ли целевая система, путем поиска файла с наименованием «/bin/lsxxxssswwdd11vv», содержащим слово «WATERDROP». В случае, если целевая система не заражена, «дроппер» перезаписывает легитимные двоичные файлы «ls», «netstat» и «crond» зараженными двоичными файлами (например, /bin/lsxxxssswwdd11vv, selfrecoverheader, mainpasteheade), а также ищет службу SSH и заражает ее вредоносной библиотекой «libsshd.so». Указанная библиотека взаимодействует с сервером управления злоумышленников и передает информацию о целевой системе. Файлы «selfrecoverheader» и «mainpasteheade» обеспечивают закрепление вредоносного программного обеспечения в целевой системе.

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

Обеспечить на уровне сетевых средств защиты информации ограничение обращений к IP-адресу 45[.]125[.]64[.]200, используя схему доступа по «черным» или «белым» спискам.

Осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
94e8540ea39893b6be910cfee0331766e4a199684b0360e367741facca74191f;
0e2ed47c0a1ba3e1f07711fb90ac8d79cb3af43e82aa4151e5c7d210c96baebb;
6d08ba82bb61b0910a06a71a61b38e720d88f556c527b8463a11c1b68287ce84.

16. Хакерской группировкой Vengeful Wolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем, во вложениях которых содержится вредоносный архив с наименованием «Документы.cab». Архив содержит документ-приманку с наименованием «Образец.rtf» и вредоносный файл с наименованием «Акт сверки взаиморасчетов по состоянию на 23.01.2025 года.exe», который является вредоносным программным обеспечением 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 осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):

5a8374d8c3635023baa69ffaf98d2c7fbf1f18fe9740282137f42ce275720049;
2d9417efc54b2eac9c797b07ee06c043a8040bf4a51c78983cd8b490d05a56e6;
d86c1cb610e958abb1e805a552ea666ddfc81cb07a204ea6fdc607a1d4028c0f.

17. Хакерской группировкой Watch Wolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лица ФССП России с тематикой «Исполнительный лист №1710646 от 03.02.2025». Во вложениях указанных писем содержится вредоносный файл с наименованием «Исполнительный лист №27186421-25 от 03.02.2025.exe», который представляет собой самораспаковывающийся архив. После запуска указанного файла осуществляется внедрение вредоносного программного обеспечения типа «бэкдор» (DarkWatchman).

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, а также заблокировать получение писем с адреса электронной почты mail@fssp[.]website.

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

4ad74aab[.]store;
4ad74aab[.]online;
hxxp[:]//4ad74aab[.]store[:]443/;
hxxp[:]//4ad74aab[.]online/index[.]php;
hxxp[:]//4ad74aab[.]online[:]443/.

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

0ad0c1d0348d526f7c84923a80a4f74c923715d9ca9fff3aebf07d81009a51a1;
1918e9aafc580711377e2cd239b9185b571db145b6d830681c87e21561508835;
f7b011a9e5c9c00b380f9645abd96c1643a0e2628a954dad7a06070c3206b4f2;
53c8d2f87e9576646d5ed60587147ef16463757ba9128282b63519d6aefaf3ad;
0ace41794e85342cbff8adbbd331b8c174b31097276f4c37f858ae805b2384a6;
ef5759af287e095b29b5843f7f5a2cce4539acfd8ac064461d32bf1db5ed5b1f;

4645d34288689ad85455b74fbcc350521fead8870a46a87f3fb2e152433e6f0d.

18. Хакерской группировкой Rare Werewolf, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от АО «Концерн КЭМЗ», во вложениях которых содержится вредоносный исполняемый файл, замаскированный под официальный документ. После запуска пользователем указанного файла осуществляется открытие документа приманки и загрузка легитимного программного обеспечения для получения удаленного доступа к целевой системе «AnyDesk».

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

bb243113d236f823abd1839025190e763fe34c40da4949b77558995cc1a07625;
2b674218337115041e1b55e5c79a9eee0da0d9e7131942265c67a4430682ac9f;
321b7473425dc9ae8ed0a1fb7e501a956df4ca3a91e310ca9523895328ddf72f.

19. Хакерскими группировками, нацеленными на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от лица сотрудника компании по продаже автомобилей из Узбекистана. Во вложениях указанных писем прикреплен архив, содержащий вредоносное программное обеспечение типа «стилер» (FromBook). После запуска пользователем указанного вредоносного программного обеспечения осуществляется обход встроенного антивирусного программного обеспечения «Windows Defender», создание запланированной задачи запуска FromBook, подключение к управляющим серверам злоумышленников, а также эксфильтрация данных целевой системы.

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:

www[.]lapostehotel[.]one;

hxxp[:]//www[.]lapostehotel[.]one/kmge/.

Также необходимо осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем

внесения в правила корреляции событий следующих индикаторов компрометации (sha256):

3c66ec3ccce10af7e58a360fbf188a1c879ad04a37c8fdc29ee7ebb75a28104f;

210c8c40bffff97e6fc7fc670e3a08d67c55307ec73295eff3d2c8b88983a02f.

20. Хакерской группировкой Mythic Likho, нацеленной на органы государственной власти и субъекты критической информационной инфраструктуры Российской Федерации, осуществляются фишинговые рассылки электронных писем от отдела кадров российской компании с тематикой «Касаемо вашего сотрудника». В тексте письма злоумышленники просят дать краткую характеристику бывшего сотрудника и прикрепляют ссылку на архив с наименованием «Резюме_ЗелибРВ.rar». Данный архив содержит еще один архив с наименованием «Резюме.rar», в который вложены файлы, замаскированные под скан-копии паспорта сотрудника, а также файл-ярлык с наименованием «Rez_ZelibRV.lnk». После открытия пользователем указанного файла-ярлыка осуществляется демонстрация документа приманки и внедрение вредоносного программного обеспечения типа «фреймворк постэксплуатации» (Merlin).

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:

hxxps[:]//mail[.]gkrzn[.]ru:443/data;

hxxps[:]//yuristconsultant[.]ru[:]443/data_query;

hxxps[:]//pop3[.]gkrzn[.]ru/data.

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

41ebd5d8a575d3ea28ad5c4ad2f04bfab29fbc98dd2d068f4d4f5b48cba1e05a;

ece4c52072ad2aebc24deb602b3184291eda536662034525ef5f1254cde0911a;

25b6adc34282fb6977f108df9b9ef99bddf1d6b671f7fdc982e2c368c5118a6b.

III. Другие угрозы информационной безопасности.

Хакерскими группировками путем подмены почтовых адресов Управления ФСТЭК России по Уральскому федеральному округу в адрес федеральных органов исполнительной власти, субъектов критической информационной инфраструктуры и организаций Российской Федерации направляются фишинговые письма, во вложениях которых находится архив с наименованием «запрос5161-2.7z». Архив содержит исполняемый файл «20250203_5_161.scr», замаскированный под официальное письмо Управления ФСТЭК России по Уральскому федеральному округу с

расширением «.pdf», который является экземпляром вредоносного программного обеспечения типа «троян» (Trojan.Win32.AntiVM.das).

С целью предотвращения реализации угроз безопасности информации, связанных с фишингом, необходимо выполнить следующие мероприятия.

1. Заблокировать доставку писем от адресов электронной почты ufo@fstec.ru, feo.ufo@fstec.ru, kii.ufo@fstec.ru, oek.ufo@fstec.ru, omto.ufo@fstec.ru, otd2_ufo@fstec.ru, otd9_ufo@fstec.ru.

2. При получении подозрительных электронных писем от имени ФСТЭК России необходимо связаться с работником ФСТЭК России и удостовериться в их легитимности.

3. Не открывать почтовые вложения форматов .7z, .rar, .zip, если заведомо не известно, что указанные вложения должны быть направлены в адрес вашего органа (организации).

4. Не открывать полученные по электронной почте файлы, использующие двойные расширения, например .pdf.exe.

5. В случае получения данного фишингового письма от указанных в пункте 1 почтовых адресов осуществить проверку инфраструктуры с использованием средств антивирусной защиты.

6. 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;

организовать получение почтовых вложений только от известных отправителей;

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

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.

7. Обеспечить на уровне сетевых средств защиты информации ограничение обращений к следующим адресам, используя схему доступа по «черным» или «белым» спискам:

hamrick[.]com;

podofo[.]sf[.]net.

8. Осуществить настройку правил системы мониторинга событий информационной безопасности (при ее наличии) путем внесения в правила корреляции событий следующих индикаторов компрометации (sha256):
a0488131f969c4f4873e24a7bbce6dabac5cb9ff80e04421140ed9f663695c98;
27967a3dcacf33a5698c419576864aa1fc5bf1a541a9d28ce15527f4e53d9bcf;
8c84b9675272ec471c3d9b1b10957bf9f8676f17a491b15099eaa9ff1625a75a;
f2406609b6424d1a9fb4e09b7e3be8c960e6e9c48e7203be0e226f3a658ea504;
f2760a8ae2c82006b14c93e2256a345b525b7caa96d50575e5e2e5f378a17abe.

9. Реализовать следующие настройки параметров безопасности почтовых серверов органа (организации) в целях исключения подмены адресов электронной почты.

9.1. Осуществить настройку параметра безопасности Sender Policy Framework (SPF) путем редактирования записей DNS-зоны сервера необходимого домена следующим образом:

добавить новую TXT-запись, которая описывает перечень DNS и IP-адресов, являющихся источниками отправки электронных сообщений. Например, следующего содержания:

example.org IN TXT "v=spf1 mx ip4:133.133.133.133 +a:smtp.mail.ru include:yandex.ru ~all"

из которой следует, что отправлять сообщения от имени домена example.org могут только сервера, указанные в mx-записях, а также IP адрес 133.133.133.133.

Расшифровка параметров:

v=spf1 является версией, всегда принимает значение spf1;

a – разрешает прием писем с адреса, который указан в A и\или AAAA записи домена отправителя;

mx – разрешает принимать письма с адреса, который указан в mx записи домена;

all – определяет, что будет происходить с письмами, которые не соответствуют установленной политике: "-" – отклонять, "+" – пропускать, "~" – дополнительные проверки, "?" – нейтрально;

include – разрешает принимать письма с серверов, разрешенных SPF-записями домена;

ip4 и ip6 – уточняющие параметры для указания конкретных адресов.

9.2. Осуществить настройку функции безопасности Domain Keys Indentfied Mail (DKIM) подписи и DNS записей путем создания пары ключей шифрования (открытый и закрытый):

openssl genrsa -out private.pem 1024 (сгенерировать закрытый ключ длинной 1024, ключи с длинной менее 1024 применять не рекомендуется);

openssl rsa -pubout -in private.pem -out public.pem (получить публичный ключ из закрытого).

Далее, необходимо указать путь к закрытому ключу в файле конфигурации почтового сервера и указать публичный ключ в конфигурации DNS путем добавления записи следующего содержания:

mail._domainkey.your.tld TXT "v=DKIM1; k=rsa; t=s; p=<публичный ключ>".

Если требуется заполнить поле TTL, то необходимо указать параметр 21600.

Расшифровка параметров:

mail – селектор. Можно указать несколько записей с разными селекторами, где в каждой записи будет свой ключ. Применяется в том случае, если задействовано несколько серверов (на каждый сервер свой ключ);

v – версия DKIM, всегда принимает значение v=DKIM1 (обязательный аргумент);

k – тип ключа, всегда принимает значение k=rsa (по крайней мере, на текущий момент);

p – публичный ключ, кодированный в base64 (обязательный аргумент);

t – флаги:

t=y – режим тестирования. Такие ключи отличаются от неподписанных и нужны лишь для отслеживания результатов;

t=s – означает, что запись будет использована только для домена, к которому относится запись. Использование указанного флага не рекомендуется, если используются субдомены.

9.3. Осуществить настройку функции безопасности Domain-based Message Authentication, Reporting and Conformance (DMARC) путем добавления TXT-записи с указанием действий сервера в случае, когда проверка подлинности DKIM и SPF не пройдена, например:

_dmarc IN TXT “v=DMARC1; p=reject; rua=mailto:dmarc@example.org; sp=reject; aspf=s; adkim=s; ri=604800“.

Расшифровка параметров:

v – версия протокола DMARC, принимает значение v=DMARC1 (обязательный параметр);

p – правило для домена. Обязательный параметр, принимает значения none, quarantine и reject, где:

none – не делает ничего, кроме подготовки отчетов;

quarantine – добавляет письмо в СПАМ;

reject – отклоняет письмо;

rua=mailto:dmarc@example.org - адрес электронной почты, на который присылаются уведомления о результатах проверки;

aspf – определяет тип проверки “strict“ для SPF-записей;

adkim – определяет тип проверки “strict“ для DKIM-подписей;

ri – интервал в секундах, определяющий, как часто получать и агрегировать XML-отчеты.