Бюллетень информационной безопасности от 01.04.2026

I. Сведения об уязвимостях.

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

1. Уязвимость инструмента мониторинга виртуальной инфраструктуры VMware Aria Operations (BDU:2026-02323, уровень опасности по CVSS 3.1 – высокий), связанная с непринятием мер по нейтрализации специальных элементов. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

2. Уязвимость файлов формата PKCS#12 библиотеки OpenSSL (BDU:2026-01223, уровень опасности по CVSS 3.1 – средний), связанная с разыменованием указателей. Эксплуатация уязвимость может позволить нарушителю вызвать отказ в обслуживании или выполнить произвольный код.

В целях предотвращения возможности эксплуатации указанных в пунктах 1-2 уязвимостей рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования обновлений безопасности программных, программно-аппаратных средств, утвержденной ФСТЭК России 28.10.2022 (далее – «Методика тестирования»), а также Методикой оценки уровня критичности уязвимостей программных, программно-аппаратных средств, утвержденной ФСТЭК России 30.06.2025 (далее – «Методика оценки») (https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty).

3. Уязвимость плагина для визуализации grafanacubism-panel платформы для мониторинга и наблюдения Grafana (BDU:2026-03177, уровень опасности по CVSS 3.1 – высокий), связанная с непринятием мер по защите структуры вебстраницы. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, раскрыть и модифицировать защищаемую информацию с помощью специально сформированного URL-адреса.

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 уровня веб-приложений для фильтрации сетевого трафика;

ограничить доступ к уязвимому программному обеспечению, используя схему доступа по «белым спискам»;

ограничить возможность пользователей перехода по ссылкам, полученным из недоверенных источников;

использовать средства антивирусной защиты для проверки ссылок, полученных из недоверенных источников;

использовать системы мониторинга и управления событиями информационной безопасности для отслеживания обращений к недоверенным сетевым адресам и доменным именам;

ограничить доступ к уязвимому программному обеспечению из внешних сетей.

4. Уязвимость текстового редактора Notepad++ (BDU:2026-02029, уровень опасности по CVSS 3.1 – высокий), связанная с использованием ненадежного пути поиска. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код при помощи специально сформированного исполняемого файла.

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:

ограничить возможность открытия файлов, полученных из недоверенных источников;

использовать средства антивирусной защиты для проверки файлов, полученных из недоверенных источников;

использовать замкнутую программную среду для работы с файлами, полученными из недоверенных источников;

использовать системы обнаружения и предотвращения вторжений для обнаружения (выявления, регистрации) и реагирования на попытки эксплуатации уязвимости.

5. Уязвимость пользовательского интерфейса Nginx UI сервера nginx (BDU:2026-02720, уровень опасности по CVSS 3.1 – критический), связанная с отсутствием аутентификации для критичной функции. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, получить несанкционированный доступ к защищаемой информации путем отправки специально сформированного GET-запроса.

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:

ограничить доступ к уязвимому программному обеспечению, используя схему доступа по «белым спискам»;

использовать системы мониторинга и управления событиями информационной безопасности для отслеживания событий, связанных с обращением к прикладному программному интерфейсу backup;

использовать виртуальные частные сети для организации удаленного доступа;

ограничить доступ к уязвимому программному обеспечению из внешних сетей.

6. Уязвимость службы snapd операционных систем Ubuntu (BDU:2026-03419, уровень опасности по CVSS 3.1 – высокий), связанная с некорректным присвоением привилегий. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии до уровня root.

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 использовать системы мониторинга и управления событиями информационной безопасности для отслеживания событий, связанных с действиями пользователей с правами root.

7. Уязвимость компонента REST WebServices диспетчера идентификации Oracle Identity Manager программной платформы Oracle Fusion Middleware и компонента Web Service Security приложения Oracle Web Services Manager (BDU:2026-03475, уровень опасности по CVSS 3.1 – критический, связанная с отсутствием аутентификации для критичной функции. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, получить несанкционированный доступ к системе путем отправки специально сформированного HTTP-запроса.

В случае невозможности установки обновления программного обеспечения рекомендуется использовать средства межсетевого экранирования уровня веб-приложений для фильтрации сетевого трафика.

8. Уязвимость текстового редактора Notepad операционных систем Windows (BDU:2026-01742, уровень опасности по CVSS 3.1 – высокий), связанная с непринятием мер по очистке данных на управляющем уровне. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

9. Уязвимость реализации протокола сетевой аутентификации NT LAN Manager (NTLM) операционных систем Windows (BDU:2023-01101, уровень опасности по CVSS 3.1 – высокий), связанная с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю обойти ограничения безопасности и повысить свои привилегии.

10. Уязвимость почтового сервера Microsoft Exchange Server (BDU:2021-04125, уровень опасности по CVSS 3.1 – критический), связанная с ошибками управления генерацией кода. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

11. Уязвимость брокера регистрации вспомогательных технологий Windows Accessibility Infrastructure (ATBroker.exe) операционных систем Windows (BDU:2026-03020, уровень опасности по CVSS 3.1 – высокий), связанная с неправильным присвоением разрешений для критичного ресурса. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии.

12. Уязвимость средства управления серверами Windows Admin Center (BDU:2026-03415, уровень опасности по CVSS 3.1 – высокий), связанная с

недостатками процедуры аутентификации. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, повысить свои привилегии.

В целях предотвращения возможности эксплуатации уязвимостей 8-12 в условиях прекращения технической поддержки производителем операционных систем Windows необходимо руководствоваться информационным сообщением ФСТЭК России от 23.10.2025 № 240/91/3526 (https://fstec.ru/dokumenty/vse-dokumenty/informatsionnye-i-analiticheskie-materialy/informatsionnoe-soobshchenie-fstek-rossii-ot) (далее — «информационное сообщение ФСТЭК России»).

13. Уязвимость системы управления базами данных Microsoft SQL Server (BDU:2026-02829, уровень опасности по CVSS 3.1 – высокий), связанная с недостатками механизма контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, повысить свои привилегии.

В целях предотвращения возможности эксплуатации данной уязвимости в условиях прекращения технической поддержки производителем операционных систем Windows необходимо руководствоваться информационным сообщением ФСТЭК России, а также принять следующие компенсирующие меры:

ограничить доступ к уязвимому программному обеспечению, используя схему доступа по «белым спискам»;

использовать системы мониторинга и управления событиями информационной безопасности для отслеживания попыток эксплуатации уязвимости;

использовать виртуальные частные сети для организации удаленного доступа;

ограничить доступ к уязвимому программному обеспечению из внешних сетей;

минимизировать пользовательские привилегии;

отключить (удалить) неиспользуемые учетные записи пользователей.

14. Уязвимость виртуальной обучающей среды Moodle (BDU:2026-02532, уровень опасности по CVSS 3.1 – критический), существующая из-за непринятия мер по защите структуры веб-страницы. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код путем создания специально сформированного запроса.

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 антивирусной защиты для отслеживания средств эксплуатации уязвимости;

минимизировать пользовательские привилегии;

отключить (удалить) неиспользуемые учетные записи пользователей.

Для отечественной операционной системы РедОС рекомендуется осуществить обновление, используя рекомендации разработчика: http://repo.red-soft.ru/redos/7.3c/x86_64/updates/.

15. Уязвимость компонента net/packet/af_packet.c ядра операционной системы Linux (BDU:2025-15791, уровень опасности по CVSS 3.1 – средний), связанная с ошибками синхронизации при использовании общего ресурса. Эксплуатация уязвимости позволяет нарушителю вызвать отказ в обслуживании.

Для отечественной операционной системы Astra Linux рекомендуется обновить пакеты linux-6.1 до 6.1.152-1.astra1+ci9, linux-6.12 до 6.12.47-1.astra1+ci8 и linux-6.6 до 6.12.47-1.astra1+ci8 или более высоких версий, используя рекомендации разработчика: https:// wiki.astralinux.ru/astra-linux-se18-bulletin-2025-1113SE18.

Для отечественной операционной системы Astra Linux рекомендуется обновить пакеты linux-5.10 до 5.10.241-1.astra1+ci48, inux-6.1 до 6.1.152-1.astra1+ci20, linux до 5.4.0-218.astra1+ci178, linux-5.15 до 5.15.0-158.astra1+ci183 или более высоких версий, используя рекомендации разработчика: https://wiki.astralinux.ru/astra-linux-se17-bulletin-2025-1202SE17.

Для отечественной операционной системы Astra Linux рекомендуется обновить пакеты linux-5.10 до 5.10.241-1.astra1+ci48, linux-6.1 до 6.1.152-1.astra1+ci20, linux до 5.4.0-218.astra1+ci178, linux-5.15 до 5.15.0-158.astra1+ci183 или более высоких версий, используя рекомендации разработчика: https://wiki.astralinux.ru/astra-linux-se47-bulletin-2025-1216SE47.

Для отечественной операционной системы Astra Linux рекомендуется обновить пакеты linux-6.1 до 6.1.152-1.astra1+ci9 и linux-6.1 до 6.1.152-1.astra1+ci9 или более высоких версий, используя рекомендации разработчика: https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0126SE38.

Для отечественной операционной системы Альт СП 10 рекомендуется осуществить обновление, используя рекомендации разработчика: https://altsp.su/obnovleniya-bezopasnosti/.

Для отечественной операционной системы Альт 8 СП рекомендуется осуществить обновление, используя рекомендации разработчика: https://altsp.su/obnovleniya-bezopasnosti/.

II. Другие угрозы информационной безопасности.

1. Зафиксированы факты участившихся попыток применения злоумышленниками методов «социальной инженерии» в отношении сотрудников органов государственной власти Российской Федерации посредством мессенджеров Telegram, Whatsapp и использования искусственного интеллекта с целью получения несанкционированного доступа к их персональным данным.

Мошенниками создаются фальшивые аккаунты должностных лиц (руководителей) для отправки подчиненным сообщений в указанных мессенджерах с фишинговыми ссылками. При переходе по указанным

ссылкам злоумышленники получают доступ к персональным данным сотрудников. Также происходит отправка видеосообщений, в которых с помощью искусственного интеллекта в официально-деловой манере сгенерирована сцена с внешностью руководителей. Данные схемы мошенничества используются злоумышленниками в том числе с целью «кражи» профиля на портале «Госуслуг».

При получении подобных сообщений необходимо:

не передавая никакой информации, прекратить диалог, не отвечать на звонки с неизвестных номеров;

не пересылать подозрительные сообщения другим сотрудникам организации;

связаться с должностным лицом, от имени которого пришло сообщение, альтернативным способом для уведомления об инциденте;

проинформировать администратора информационной безопасности своей организации и Министерство цифрового развития и связи Алтайского края о попытках использования фейковых аккаунтов должностных лиц.

2. Специалистами ФСТЭК России поведен анализ результатов проведения в 2025 году эксперимента по повышению уровня защищенности государственных информационных систем федеральных органов исполнительной власти и подведомственных им учреждений, полученных в соответствии с постановлением Правительства Российской Федерации от 26.03.2025 № 372 «О проведении эксперимента по повышению уровня защищенности государственных информационных систем федеральных органов исполнительной власти и подведомственных им учреждений». По результатам проведенного анализа выявлены типовые организационные и технические недостатки информационных (автоматизированных) систем, наличие которых создает предпосылки к реализации угроз безопасности информации. Рекомендации по устранению типовых организационных и технических недостатков информационных (автоматизированных) систем представлены в Приложении 3 к настоящему бюллетеню.

3. Анализ сведений об угрозах безопасности информации, проводимый специалистами ФСТЭК России в условиях сложившейся обстановки, показывает, что хакерскими группировками при осуществлении целевых компьютерных атак на информационную инфраструктуру органов (организаций) активно эксплуатируются уязвимости сервисов и недостатки конфигурации сетевых (пограничных) устройств (межсетевых экранов, пограничных маршрутизаторов, аппаратных VPN-шлюзов, аппаратных средств обнаружения и предотвращения вторжений, прокси-серверов), находящихся на внешнем периметре информационной инфраструктуры органа (организации).

Рекомендуется провести контроль реализации принятых мер по защите периметра информационных (автоматизированных) систем в соответствии с требованиями о защите информации, установленными статьей 16 Федерального закона от 27.07.2006 № 149 ФЗ «Об информации,

информационных технологиях и о защите информации», в частности, для информационных (автоматизированных) систем, взаимодействующих с сетью «Интернет», с учетом особенностей их функционирования. Организационные и технические меры по повышению защищенности внешнего периметра органа (организации) представлены в Приложении 4 к настоящему бюллетеню.

4. Анализ сведений об угрозах безопасности информации, проводимый специалистами ФСТЭК России в условиях сложившейся обстановки, показывает, что в настоящее время для получения несанкционированного доступа к информационной инфраструктуре органов государственной власти и субъектов критической информационной инфраструктуры Российской Федерации злоумышленниками активно применяются различные методы реализации компьютерных атак, такие как целевой «фишинг», «AitM-фишинг», «ClickFix», поддельные «CAPTCHA», «SEO-отравление», «Supply-chain» атаки, «FastFlux», «DoubleFlux».

С целью повышения защищенности информационных ресурсов органов государственной власти и субъектов критической информационной инфраструктуры Российской Федерации необходимо принять следующие дополнительные меры защиты информации.

1. Для предотвращения реализации угроз безопасности информации, связанных с деятельностью злоумышленников по целевым «фишинговым» рассылкам, необходимо:

1.1. Производить на этапе приема письма почтовым сервером автоматическую проверку вложений с использованием публичных или имеющихся «песочниц» («sandbox») для выявления вредоносной активности.

1.2. 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.

1.3. Осуществлять автоматическую проверку указанных в письмах URL-адресов, содержащихся в электронных письмах, с использованием механизмов анализа ссылок.

1.4. Отключить автоматическую загрузку внешнего содержимого (например, изображений, скриптов) в почтовых клиентах.

1.5. 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.

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

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

1.8. 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 исключить работу под учетной записью root, при необходимости осуществить настройку необходимого перечня команд в файле конфигураций sudoers. Использовать для разграничения прав доступа к файлам и директориям как отдельных пользователей, так и групп пользователей команды chmod, chown, chgrp.

1.9. Создать отдельный электронный почтовый адрес, на который пользователи информационной инфраструктуры будут присылать письма, которые могут содержать вредоносное содержание (ссылку или вложение).

1.10. Проинформировать пользователей информационной инфраструктуры о необходимости безопасной работы с электронной почтой, а именно:

внимательно проверять адрес отправителя, даже в случае совпадения имени с уже известным контактом;

не открывать письма от неизвестных адресатов;

проверять письма, в которых содержатся призывы к действиям (например, «открой», «прочитай», «ознакомься»), а также с темами про финансы, банки, геополитическую обстановку или угрозы;

не переходить по ссылкам, которые содержаться в электронных письмах, особенно если они длинные или наоборот, используют сервисы сокращения ссылок (bit.ly, tinyurl.com и т.д.);

не нажимать на ссылки из письма, если они заменены на слова, не наводить на них мышкой и просматривать полный адрес сайтов;

проверять ссылки, даже если письмо получено от другого пользователя информационной инфраструктуры;

не открывать вложения, особенно если в них содержатся документы с макросами (при необходимости реализовать запрет на их выполнение), архивы с паролями, а также файлы с расширениями RTF, LNK, CHM, VHD;

внимательно относиться к письмам на иностранном языке, с большим количеством получателей и орфографическими ошибками;

в случае появления сомнений – направлять полученное письмо как вложение администратору информационной инфраструктуры.

1.11. Активировать механизмы проверки электронной почты, проверки подлинности домена-отправителя (использовать технологии DKIM, DMARC, SPF, DNS BL), а также настроить проверку входящих писем с использованием этих технологий согласно рекомендациям по базовой настройке механизмов безопасности почтовых сервисов от атак, связанных с подменой отправителя (спуфинг-атак) (https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rekomendatsii-po-bazovoj-nastrojke-mekhanizmov-bezopasnosti-pochtovykh-servisov-ot-atak-svyazannykh-s-podmenoj-otpravitelya-spufing-atak).

1.12. Заблокировать получение пользователями информационной инфраструктуры в электронных письмах вложений с расширениями ADE, ADP, APK, APP, APPX, ASP, APPXBUNDLE, BAS, BAT, BIN, CAB, CHM, CLA, CLASS, CMD, CNT, COM, CPL, CRT, CSH, DLL, DMG, DRV, EX, EX_, EXE, FXP, GADGET, GRP, HLP, HPJ, HTA, INF, INK, INS, ISP, ISO, ITS, JAR, JS, JSE, KSH, LIB, LNK, MAD, MAF, MAG, MAM, MAQ, MAR, MAS, MAT, MAU, MAV, MAW, MCF, MDA, MDB, MDE, MDT, MDW, MDZ, MSC, MSH, MSHXML, MSH1, MSH1XML, MSH2, MSH2XML, MSI, MSIX, MSIXBUNDLE, MSP, MST, NLM, NSH, OCX, OPS, OSD, OVL, PCD, PIF, PL, PLG, PRF, PRG, PS1, PS1XML, PS2, PS2XML, PSC1, PSC2, PST, REG, RTF, SCF, SCR, SCT, SH, SHB, SHS, SYS, VB, VBA, VBE, VBP, VBS, VHD, VSMACROS, VSW, VXD, WS, WSC, WSF, WSH, XBAP, XNK.

1.13. Обеспечить своевременное обновление программного обеспечения почтовых серверов, почтовых шлюзов и компонентов почтовой инфраструктуры, а также проведение регулярной проверки наличия уязвимостей и корректности настроек для исключения их эксплуатации злоумышленниками в соответствии с Методикой тестирования.

2. Для предотвращения реализации угроз безопасности информации, связанных с деятельностью злоумышленников по фишинговым рассылкам с применением тактики перехвата аутентификационных данных («AitM-фишинг»), необходимо:

2.1. Обеспечить применение многофакторной аутентификации для учетных записей пользователей, имеющих доступ в сеть «Интернет».

2.2. Обеспечить регистрацию событий аутентификации, выданных токенов доступа, успешных и неуспешных попыток входа, а также попыток входа с удаленных, заблокированных учетных записей пользователей для осуществления мониторинга и выявления аномальной активности.

2.3. По возможности использовать системы мониторинга и управления событиями информационной безопасности (далее – SIEM-системы).

2.4. Ограничить использование устаревших протоколов аутентификации (например, NTLMv1, POP3, IMAP без TLS).

3. Для предотвращения реализации угроз безопасности информации, связанных с деятельностью злоумышленников, применяющих методы «ClickFix» и поддельные «CAPTCHA», необходимо:

3.1. Ограничить выполнение команд оболочки сценариев «PowerShell» и «командной строки» через групповые политики и «белые» списки приложений. При необходимости проведения работ с использованием указанных утилит необходимо реализовать проверку действий пользователей информационной инфраструктуры путем написания правил корреляции событий (например, Sigma-правил) для SIEM-систем. Обеспечить мониторинг и анализ событий безопасности, детектируемых таким образом.

3.2. Ограничить запуск системных инструментов wscript.exe и mshta.exe с задействованием объектов групповой политики имеющихся средств антивирусной защиты.

3.3. Осуществлять мониторинг событий, связанных с хранением в буфере обмена аномального программного кода.

3.4. Использовать средства обнаружения и реагирования на уровне узла для нейтрализации угроз безопасности информации, связанных с выполнением вредоносного программного кода.

3.5. Ограничить выполнение программного кода в операционной системе для пользователей информационной инфраструктуры.

3.6. Отключить комбинацию клавиш «Win+R» на конечных точках.

4. Для предотвращения реализации угроз безопасности информации, связанных с деятельностью злоумышленников, применяющих метод продвижения вредоносных сайтов в начало поисковой выдачи («SEO-отравление»), необходимо:

4.1. Запретить пользователям информационной инфраструктуры самостоятельную установку программного обеспечения или его обновлений. Проинформировать пользователей об обязанности обращения в подразделение, ответственное за внедрение информационных технологий, в случае необходимости установки программного обеспечения или его обновления.

4.2. Использовать средства антивирусной защиты для проверки адресов сайтов на вредоносную активность.

4.3. Использовать системы анализа сетевого трафика (NTA) и обеспечить их интеграцию со средствами антивирусной защиты.

4.4. Проинформировать пользователей о запрете перехода по рекламным ссылкам.

5. Для предотвращения реализации угроз безопасности информации, связанных с деятельностью злоумышленников, осуществляющих атаки на

цепочку поставок («Supply-chain» атаки), необходимо принять следующие меры защиты.

5.1. Осуществлять проверку обновлений программного обеспечения, в соответствии с Методикой тестирования.

5.2. Осуществлять обновления из доверенных источников.

5.3. Организовать централизованные серверы обновлений внутри информационной инфраструктуры, исключая прямое получение обновлений с внешних ресурсов рабочими станциями пользователей.

5.3. Отслеживать обновления безопасности на официальном сайте производителя.

5.4. Отслеживать публичные и стабильные версии в репозиториях в случае использования программного обеспечения с открытым исходным кодом.

6. Для предотвращения реализации угроз безопасности информации, связанных с деятельностью злоумышленников, применяющих методы сокрытия сетевой инфраструктуры («FastFlux» и «DoubleFlux»), необходимо принять следующие меры защиты.

6.1. Использовать средства антивирусной защиты и осуществлять своевременную настройку межсетевых экранов по блокировке вредоносных сетевых индикаторов. Использовать каналы сбора данных и инструменты контроля и формирования информации для выявления известных доменов «FastFlux» и связанных с ними IP-адресов.

6.2. Обеспечить осуществление подключения к внешним сайтам только с использованием безопасного протокола HTTPS.

6.3. Применять системы обнаружения вторжений для выявления аномальных доменов с нестабильной DNS-историей, для блокировки подозрительных ASN, детектирования частых DNS-запросов к доменам, которые часто меняют свой IP-адрес, а также для блокировки подозрительных DNS-резолверов.

6.4. Организовать анализ и мониторинг NS-записей на предмет их частой смены (более 2 раз в час) и на принадлежность разным ASN.

6.5. Обеспечить проверку IP-адреса авторитетного DNS-сервера на предмет отнесения к сетям российского провайдера, частой смены, принадлежности разным странам.

6.6. Отслеживать время, в течении которого хранится результат разрешения имени в кэше DNS-резолвера (при атаках «FastFlux», указанное время менее 5 минут).

6.7. Ограничить возможность прямых DNS-запросов к внешним резолверам, разрешив использование только утвержденных внутренних DNS-серверов. Для используемых DNS-серверов обеспечить возможность блокировки вредоносных доменов с помощью механизма DNS Sinkholing.

7. Для предотвращения реализации угроз безопасности информации, связанных с внедрением вирусов-шифровальщиков через почтовые вложения, а также после получения несанкционированного доступа к информационной инфраструктуре посредством эксплуатации уязвимостей веб-сайтов и средств, находящихся на периметре информационной инфраструктуры, необходимо:

7.1. Обеспечить резервирование информации, обрабатываемой в информационной инфраструктуре, и проверить наличие актуальных резервных копий.

7.2. Обеспечить хранение резервных копий в изолированном от сети «Интернет» сегменте информационной инфраструктуры.

7.3. Ограничить доступ пользователей информационной инфраструктуры к резервным копиям данных.

7.4. Ограничить (при возможности) сетевое взаимодействие между сегментами информационной инфраструктуры по принципу «запрещено все, что явно не разрешено» (например, с помощью технологии VLAN и списков контроля доступа сетевого оборудования).

7.5. По возможности использовать системы мониторинга сетевого трафика и выявления подозрительной активности, а также автоматической блокировки потенциальных угроз.

7.6. Запретить пользователям подключать к автоматизированным рабочим местам неучтенные машинные носители информации, мобильные устройства и открывать ссылки из почтовых сообщений, бесконтрольно скачивать файлы из сети «Интернет», а также использовать мобильные устройства для подключения к сети «Интернет».

7.7. Ограничить посредством прокси-сервера список внешних информационных ресурсов, к которым пользователи информационной инфраструктуры могут получить доступ (например, путем введения «белых» списков информационных ресурсов, к которым разрешен доступ).

7.8. Организовать доступ к удаленным сегментам информационной инфраструктуры (при их наличии) с применением виртуальных частных сетей (VPN-сетей).

7.9. Обеспечить применение средств антивирусной защиты и антиспама, а также своевременное обновление их баз данных.

7.10. Использовать средства обнаружения и реагирования на конечных узлах для выявления попыток массового шифрования файлов и подозрительной активности процессов.

7.11. Разработать и утвердить порядок реагирования на инциденты, связанные с распространением вредоносным программным обеспечением типа «шифровальщик», включающий процедуры изоляции узлов, уведомления ответственных лиц и восстановления из резервных копий.