**МИНИСТЕРСТВО
ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ
РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНЦИФРЫ РОССИИ)**

ЗАМЕСТИТЕЛЬ МИНИСТРА

Пресненская наб., д.10, стр.2, Москва, 123112
Справочная: +7 (495) 771-8000

_____ № _____

на № _____ от _____

Комитет Совета Федерации
по экономической политике
Федерального Собрания
Российской федерации

В соответствии с письмами Комитета Совета Федерации по экономической политике Федерального Собрания Российской федерации от 16 ноября 2022 г. № 3.6-14/4546@ и от 21 ноября 2022 г. № 3.6-14/4618@ Минцифры России направляет материалы для «круглого стола» на тему «О ходе реализации Указа Президента Российской Федерации от 30 марта 2022 года № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» в части импортозамещения программного обеспечения и оборудования».

В целях реализации Указа Президента Российской Федерации от 30 марта 2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» (далее – Указ № 166) принято постановление Правительства Российской Федерации от 22 августа 2022 г. № 1478 «Об утверждении требований к программному обеспечению, в том числе в составе программно-аппаратных комплексов, используемому органами государственной власти, заказчиками, осуществляющими закупки в соответствии с Федеральным законом «О закупках товаров, работ, услуг отдельными видами юридических лиц» (за исключением организаций с муниципальным участием), на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации, Правил согласования закупок иностранного программного обеспечения, в том числе в составе программно-аппаратных комплексов, в целях его использования заказчиками, осуществляющими закупки в соответствии с Федеральным законом «О закупках товаров, работ, услуг отдельными видами юридических лиц» (за исключением организаций с муниципальным участием), на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации, а также закупок услуг, необходимых для использования этого программного обеспечения на таких объектах, и Правил перехода на преимущественное использование российского программного обеспечения, в том числе в составе программно-аппаратных комплексов, заказчиками, осуществляющими закупки в соответствии

с Федеральным законом «О закупках товаров, работ, услуг отдельными видами юридических лиц» (за исключением организаций с муниципальным участием), на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации» (далее – ПО, КИИ, заказчики, постановление № 1478).

Постановлением № 1478 утверждены требования к ПО, используемому заказчиками на принадлежащих им значимых объектах КИИ (далее –Требования), правила согласования закупок иностранного ПО на таких объектах и правила перехода на преимущественное использование российского ПО.

Согласно Требованиям ПО, используемое на принадлежащих органам государственной власти и заказчикам значимых объектах КИИ, должно быть включено в единый реестр российских программ для электронных вычислительных машин и баз данных или в единый реестр программ для электронных вычислительных машин и баз данных из государств – членов Евразийского экономического союза, за исключением Российской Федерации.

При этом в случае необходимости осуществления закупок иностранного ПО и необходимых для его использования услуг для целей их использования на значимых объектах КИИ такие закупки заказчикам в соответствии с подпунктом «а» пункта 1 Указа № 166 необходимо согласовать с уполномоченным в соответствии с постановлением Правительством Российской Федерации от 22 августа 2022 г. № 1478 федеральным органом исполнительной власти .

Во исполнение пункта 4 постановления № 1478 Минцифры России разработан проект методических рекомендаций по переходу на использование российского ПО, в том числе на значимых объектах КИИ (далее – Методические рекомендации), включающий в том числе рекомендации в части целевых показателей, сроков перехода субъектов КИИ, а также иных органов и организаций на использование российского ПО (в разрезе классов ПО), а также перечень мероприятий в области организационного и нормативного обеспечения процесса указанного перехода.

После согласования ФСБ России и ФСТЭК России Методические рекомендаций будут утверждены Минцифры России.

Дополнительно сообщаем, что в развитие норм, установленных Указом № 166, Минцифры России разработан проект федерального закона, устанавливающий требования для субъектов КИИ преимущественного использования российского ПО, телекоммуникационного оборудования и радиоэлектронной продукции на значимых объектах КИИ. Проектом федерального закона в том числе предусматривается введение механизмов лицензирования деятельности по реализации ПО, происходящего из иностранных государств. Проектом федерального закона также предусмотрено, что Правительство Российской Федерации устанавливает сроки и порядок перехода субъектов КИИ на преимущественное использование российского ПО, телекоммуникационного оборудования и радиоэлектронной продукции на принадлежащих им значимых объектах КИИ.

В части абзаца 2 подпункта «б» пункта 2 Указа № 166 об определении сроков и порядка перехода субъектов КИИ на преимущественное применение доверенных

программно-аппаратных комплексов на принадлежащих им значимых объектах КИИ сообщаем, что Минпромторгом России разработан проект постановления Правительства Российской Федерации «О порядке перехода субъектов критической информационной инфраструктуры на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры» (далее – Проект постановления), в рамках которого утверждаются сроки и порядок перехода субъектов КИИ на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах КИИ. Проект постановления проходит процедуры согласования.

В части абзаца 3 подпункта «б» пункта 2 Указа № 166 об обеспечении внесения в законодательство Российской Федерации изменений в соответствии с настоящим Указом письмом Минцифры России от 20 мая 2022 г. № АЗ-П29-103-26373 направлен проект постановления Правительства Российской Федерации «Об утверждении требований к радиоэлектронной продукции и телекоммуникационному оборудованию, используемых заказчиками, осуществляющими закупки в соответствии с Федеральным законом «О закупках товаров, работ, услуг отдельными видами юридических лиц» (за исключением организаций с муниципальным участием), на принадлежащих им значимых объектах критической информационной инфраструктуры, и правил согласования закупок иностранных радиоэлектронной продукции, телекоммуникационного оборудования и услуг (работ), с ними связанных». До настоящего времени позиция Минпромторга России не поступала.

В части абзаца 4 подпункта «б» пункта 2 Указа № 166 об обеспечении создания и организации деятельности научно-производственного объединения, специализирующегося на разработке, производстве, технической поддержке и сервисном обслуживании доверенных программно-аппаратных комплексов для КИИ письмом Минцифры России от 27 августа 2022 г. № АШ-П25-2-226-61025 направлены предложения в части применения созданных индустриальных центров по направлениям, применения функционала центра тестирования ПО и радиоэлектронной продукции на базе ФГАУ «НИИ «Восход», а также учета предложения по применению отечественных технологий и решений при планировании НИР и НИОКР.

В части абзаца 5 подпункта «б» пункта 2 Указа № 166 предложения Минпромторга России об организации подготовки и переподготовки кадров в сфере разработки, производства, технической поддержки и сервисного обслуживания радиоэлектронной продукции и телекоммуникационного оборудования в Минцифры России не поступали.

В части абзаца 6 подпункта «б» пункта 2 Указа № 166 и пункта 2 перечня поручений Заместителя Председателя Правительства Российской Федерации Д.Н. Чернышенко от 4 апреля 2022 г. № ДЧ-П10-5417 в части создания системы мониторинга и контроля в названной сфере письмом Минцифры России от 1 августа 2022 г. № АЗ-П29-103-45084 направлены предложения по обеспечению мониторинга и контроля в рамках методических рекомендаций по цифровой

трансформации государственных корпораций и ведомственных программ цифровой трансформации федеральных органов исполнительной власти. В частности, Президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни условий ведения предпринимательской деятельности под председательством Заместителя Председателя Правительства Российской Федерации Д.Н. Чернышенко одобрены изменения в методические рекомендации по цифровой трансформации государственных корпораций и компаний с государственным участием, в соответствии с которыми учтены требования к использованию радиоэлектронной продукции отечественного производства. Данные требования являются обязательным для большинства акционерных обществ с государственным участием, включенных в специальный перечень, утвержденный распоряжением Правительства Российской Федерации от 23 января 2003 г. № 91-р.

Кроме того, Минцифры России в рамках реализации эксперимента по предоставлению права использования программ для электронных вычислительных машин, алгоритмов, баз данных и документации к ним, в том числе исключительное право на которые принадлежит Российской Федерации, на условиях открытой лицензии и созданию условий для использования открытого программного обеспечения, проводимого в соответствии с постановлением Правительства Российской Федерации от 10.10.2022 № 1804, а также в целях обеспечения технологической независимости и безопасности, в том числе в сфере КИИ, разработан проект методических рекомендаций по обеспечению информационной безопасности при создании и эксплуатации репозиториев ПО в процессе их жизненного цикла (прилагаются).

Утверждение указанных методических рекомендаций позволит установить необходимые высокие требования к качеству и обеспечению информационной безопасности в отношении публикуемого и распространяемого открытого ПО, в том числе исключительное право на которое принадлежит Российской Федерации, а также в отношении инфраструктуры отечественных репозиториев ПО.

Приложение: на 4 л. в 1 экз.

М.В. Паршин

Некрасова Ксения Олеговна
Департамент развития отрасли
информационных технологий
+7 (495) 870-29-21 (доб. 44584)

ПРОЕКТ

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по обеспечению информационной безопасности при создании и эксплуатации репозиториев программного обеспечения в процессе их жизненного цикла

I. Термины и определения

Репозиторий программного обеспечения – совокупность информационных систем, обеспечивающая разработку, хранение и сопровождение исходных текстов и объектных кодов программного обеспечения с управлением их версиями, отслеживание изменений, сборку программных продуктов, проведение их тестирования, организацию совместной работы над программным кодом, сохранность и актуальность содержимого репозитория, возможность международного взаимодействия, доступная для использования физическими и юридическими лицами без ограничений по национальному, территориальному и иным признакам, не предусмотренным законодательством Российской Федерации;

Разработчик репозитория – гражданин или юридическое лицо, выполняющие работы по разработке (включая анализ требований, проектирование, приемочные испытания) в процессе жизненного цикла репозиториев программного обеспечения;

Оператор репозитория – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации репозитория программного обеспечения, в том числе по обработке информации, содержащейся в его базах данных;

Атака на цепочку поставок – атака на информационную инфраструктуру организации путем реализации уязвимостей и технических недостатков приложений, входящих в ее состав.

II. Общие положения

1. Настоящие Методические рекомендации по обеспечению информационной безопасности при создании и эксплуатации репозиториев программного обеспечения в процессе их жизненного цикла (далее – Методические рекомендации) разработаны в соответствии с пунктом 5.2.23 Положения о Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации, утвержденного постановлением Правительства Российской Федерации от 02.06.2008 № 418.

2. Настоящие Методические рекомендации определяют базовый перечень организационных и технических мероприятий, которые рекомендовано реализовать в репозиториях программного обеспечения (далее – репозитории), для противодействия угрозам безопасности информации.

3. При реализации мероприятий по созданию, развитию, вводу в эксплуатацию, эксплуатации и выводу из эксплуатации репозиториев должны в соответствии с действующим законодательством выполняться требования о защите

информации, содержащейся в системах, устанавливаемые федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

4. Функционирование репозиториев рекомендуется осуществлять на технических средствах, находящихся на территории Российской Федерации.

5. Разработчикам и операторам репозиториев рекомендуется предусмотреть выделение вычислительных ресурсов, необходимых для реализации требований по обеспечению информационной безопасности, и обеспечить реализацию данных требований.

6. Операторам репозиториев рекомендуется разработать базовый документ, определяющий подход к управлению информационной безопасностью репозитория, устанавливающий принципы обеспечения информационной безопасности для всех участников репозитория, определяющий процесс управления уязвимостями в программном обеспечении (далее – ПО), размещенном в репозитории, и регламентирующий взаимодействие участников репозитория.

III. Меры по обеспечению информационной безопасности инфраструктуры репозитория

7. В составе информационной инфраструктуры репозитория рекомендуется предусмотреть средства защиты информации, средства сборки ПО, безопасного хранения ПО, средства разработки и тестирования ПО.

8. В инфраструктуре репозитория рекомендуется:

8.1. Реализовать идентификацию и аутентификацию пользователей;

8.2. Предусмотреть управление доступом с выделением ресурсов для всех пользователей репозитория, включая разграничение доступа к библиотекам исходного кода и объектным файлам для разных разработчиков ПО с обеспечением защиты прав на интеллектуальную собственность в соответствии с правовым статусом ПО;

8.3. Предусмотреть изоляцию среды разработки и тестирования для каждого разработчика или группы разработчиков ПО;

8.4. Предусмотреть сетевую защиту (межсетевое экранирование, обнаружение и защита от вторжений);

8.5. Реализовать применение не менее двух средств антивирусной защиты от различных поставщиков;

8.6. Обеспечить периодическое резервное копирование информации на резервные машинные носители информации;

8.7. Реализовать применение технологий, направленных на обеспечение отказоустойчивости инфраструктуры репозитория, а также средств, снижающих риски атак на цепочку поставок.

9. Перед вводом репозитория в эксплуатацию разработчику репозитория рекомендуется составить регламент проведения мероприятий по тестированию на проникновение и анализу уязвимостей в отношении компонентов репозитория.

Мероприятия по тестированию на проникновение рекомендуется провести разработчику репозитория перед вводом репозитория в эксплуатацию. В дальнейшем мероприятия по тестированию на проникновение рекомендуется проводить оператору репозитория в соответствии с разработанным регламентом проведения мероприятий по тестированию на проникновение и анализу уязвимостей в отношении компонентов репозитория, но не реже раза в год. Мероприятия по анализу уязвимостей программного обеспечения компонентов репозитория рекомендуется проводить оператору репозитория на постоянной основе. В качестве компонентов рассматриваются: общесистемное (общее), прикладное, специальное ПО, технические средства, сетевое (коммуникационное, телекоммуникационное) оборудование, средства защиты информации.

10. Оператору репозитория рекомендуется организовать обмен информацией о выявленных уязвимостях в ПО, размещенном в репозитории, с ФСТЭК России (в соответствии с регламентом включения информации об уязвимостях программного обеспечения и программно-аппаратных средств в банк данных угроз безопасности информации ФСТЭК России) и ФСБ России, а также разработать соответствующий регламент.

11. Оператору репозитория рекомендуется разработать и довести до всех пользователей репозитория регламент, определяющий порядок вывода репозитория из эксплуатации, содержащий:

11.1. Основания для вывода репозитория из эксплуатации;

11.2. Перечень и сроки реализации мероприятий по выводу репозитория из эксплуатации;

11.3. Сроки, режим хранения и дальнейшего использования ПО, размещенного в репозитории, включая порядок обеспечения доступа к ПО, размещенного в выводимом из эксплуатации репозитории, и обеспечения защиты ПО, размещенном в выводимом из эксплуатации репозитории. При этом оператору репозитория рекомендуется предусмотреть возможность передачи ПО, размещенного в репозитории, и документации на него для размещения в ином репозитории ПО, выполняющем положения настоящих методических рекомендаций;

11.4. Сроки и способы информирования пользователей о выводе репозитория из эксплуатации.

IV. Меры по обеспечению информационной безопасности программного обеспечения, размещаемого в репозитории

12. Оператору репозитория рекомендуется реализовать в составе инфраструктуры репозитория следующие сервисы, доступные для пользователей репозитория:

12.1. Сервис анализа программного обеспечения на соответствие требованиям информационной безопасности по исходным текстам методами автоматизированного

статического, динамического и композиционного анализа исходных текстов. Также в состав указанного сервиса рекомендуется включить средства фаззинг-тестирования, средства автоматизированной оценки защищённости от наиболее опасных и распространенных типов атак и уязвимостей, средства по контролю и безопасному хранению секретов. Указанный сервис обеспечивает формирование отчетов о программных дефектах и потенциальных уязвимостях в программном обеспечении, размещенном в репозитории. Конкретный состав средств, входящих в состав указанного сервиса, рекомендуется определить разработчику репозитория до ввода репозитория в эксплуатацию;

12.2. Сервис по выявлению уязвимостей информационной безопасности в ПО, размещенном в репозитории, реализуемый в рамках публичной, доступной для неограниченного числа экспертов и исследователей программного обеспечения (граждан Российской Федерации) программы по поиску уязвимостей. Порядок предоставления указанного сервиса определяется оператором репозитория в соответствии с разработанным регламентом. Указанный сервис должен быть доступен для всего ПО, размещенного в репозитории, с момента его размещения и далее на постоянной основе;

12.3. Сервис безопасной разработки ПО, предполагающий обеспечение разработчиков отечественными компиляторами, средами разработки под отечественные процессоры, эмуляторами отечественной электронной компонентной базы, инструментами тестирования безопасности ПО, либо их иностранными аналогами, в случае отсутствия отечественных решений.

13. Оператору репозитория на постоянной основе рекомендуется:

13.1. Осуществлять выявление вредоносного ПО в размещаемом в репозитории ПО с применением средств антивирусной защиты;

13.2. Осуществлять контроль целостности обрабатываемых в репозитории файлов ПО (для финальных сборок, подлежащих публикации), компиляторов и интерпретаторов (путем проверки электронных цифровых подписей и хеш-функций, а также актуального статуса цепочки сертификатов);

13.3. Вести рейтинг безопасности размещаемого в репозитории ПО, в котором указывается объем и время (периодичность) проведенного анализа в соответствии с подпунктами 12.1-12.3 и подпунктами 13.1, 13.2 настоящих Требований.