Федеральное государственное бюджетное научное учреждение
«ТОМСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ МЕДИЦИНСКИЙ ЦЕНТР РОССИЙСКОЙ АКАДЕМИИ НАУК»
(Томский НИМЦ)

Р А С П О Р Я Ж Е Н И Е

18.08.2025 № 44

Томск

О мерах по повышению защищенности информационной инфраструктуры

В соответствии с письмом Минобрнауки России от 05.08.2025г. № МН-19/955 «О мерах по повышению уровня защищенности информационной инфраструктуры Российской Федерации» для обеспечения информационной безопасности информационных (автоматизированных) систем,

ПРЕДЛАГАЮ:

1. Руководителям филиалов при организации взаимодействия с подрядной организацией выполнить следующие мероприятия.

1.1. При планировании мероприятий по взаимодействию (организации взаимодействия) с подрядными организациями необходимо:

1.1.1. Определить в рамках договорных отношений ответственность подрядных организаций за защиту информации при реализации удаленного доступа их работников к информационной инфраструктуре филиала.

1.1.2. Запросить список работников подрядной организации, планирующих осуществлять удаленный доступ к информационной инфраструктуре подрядной организации. В случае изменения состава указанных работников подрядной организации необходимо требовать от подрядной организации уведомления о фактах таких изменений в течении 1 календарного дня.

1.1.3. Определить перечень информации и информационных ресурсов, расположенных на серверах информационных систем, к которым будет предоставляться удаленный доступ работникам подрядных организаций, а также каналы связи, используемые для этих целей.

1.1.4. Запросить у подрядной организации политики информационной безопасности подрядной организации, результаты внутренних (внешних) аудитов информационной безопасности, результаты тестирования на проникновение инфраструктуры, план реагирования на компьютерные инциденты, а также регламент действий работников в случае нештатных ситуаций.

1.1.5. Определить контакты ответственных лиц по обеспечению информационной безопасности в подрядной организации и в филиале, каналы для оперативного взаимодействия (резервные каналы взаимодействия), а также порядок такого взаимодействия. Для взаимодействия организации и подрядной организации должны использоваться не персонализированные каналы взаимодействия.

1.1.6. Предусмотреть в рамках договорных отношений с подрядной организацией положения об обязанности подрядной организации уведомлять заказчика о наступлении в ее инфраструктуре компьютерных инцидентов.

1.1.7. Организовать в рамках договорных отношений выполнение подрядной организацией пункта 1.2 настоящих рекомендаций.

1.2. При взаимодействии по ранее заключенным договорам (государственным контрактам) с подрядными организациями необходимо:

1.2.1. Проинформировать подрядные организации, осуществляющие удаленный доступ к информационной инфраструктуре филиала, о необходимости реализации следующих базовых мер по информационной безопасности в собственной инфраструктуре:

- двухфакторная аутентификация пользователей;
- антивирусная защита автоматизированных рабочих мест и серверов;
- защищенное удаленное подключение с использованием средств криптографической защиты информации;
- защита почтовых сервисов от фишинга;
- защищенный обмен файлами и информацией через файловое хранилище;
- обеспечение процесса управления уязвимостями;
- реализация парольной политики (длина пароля должна быть не менее 10 символов, пароль должен содержать буквы верхнего и нижнего регистра (А-Я, A-Z, а-я, a-z), специальные символы (!, », №, %, *, /), в пароле не должно быть персонифицированной информации (имен, адресов, даты рождения, телефонов)).

1.2.2. Ограничить количество учетных записей подрядных организаций, с которых осуществляется удаленный доступ к информационной инфраструктуре филиала.

1.2.3. Учетные записи работников подрядных организаций для доступа в информационную систему должны иметь минимально необходимые права доступа, позволяющие выполнять их должностные обязанности. При увольнении или завершении выполнения работ по заключенным с подрядной организацией договорам (государственным контрактам) учетные записи работников подрядной организации должны быть удалены.

1.2.4. Обеспечить проверку и фиксацию местоположения удаленного доступа работников подрядной организации, с указанием адреса (например, IP-адрес, страна) и формата такого подключения (например, локально или удаленно).

1.2.5. Организовать реализацию подрядной организацией записи всех действий пользователей при осуществлении удаленного подключения к инфраструктуре филиала. Рекомендуемый срок хранения журналов событий не менее 1 года. Обязать подрядную организацию в случае возникновения инцидента предоставлять указанные журналы событий.

1.2.6. Обеспечить ограничение подключений к инфраструктуре организации работников подрядной организации вне рабочего времени. В случае необходимости такие подключения должны быть согласованы с филиалом.

1.2.7. Обеспечить (по возможности) включение информационной инфраструктуры подрядной организации в контур мониторинга информационной безопасности филиала (при ее наличии). Обеспечить выявление и реагирование на события информационной безопасности (многократные попытки аутентификации, сетевое сканирование, несанкционированные подключения), инициируемые

информационной инфраструктурой подрядной организации и учетными записями, с которых осуществляется удаленный доступ.

1.2.8. Производить периодические проверки подрядной организации на предмет возникновения нештатных ситуаций или инцидентов информационной безопасности путем имитации указанных событий (проведение тренировок).

1.2.9. Запретить использование подрядными организациями программного обеспечения для удаленного управления автоматизированным рабочим местом (например, TeamViewer, AnyDesk, AmmyAdmin, AeroAdmin, Radmin, LiteManager, Удаленный рабочий стол Chrome, Microsoft Remote Assistance, Microsoft Remote Desktop).

1.2.10. Удаленный сетевой доступ должен осуществляться с применением средств криптографической защиты информации, при этом обмен ключами шифрования необходимо осуществлять по алгоритмам, исключающим их раскрытие сторонним лицам. Маршруты сетевого трафика не должны проходить по сторонним сетям в незашифрованном виде. Перечень IP-адресов, с которых может осуществляться подключение, должен контролироваться средствами межсетевого экранирования.

1.2.11. Для доступа к информационной инфраструктуре организации должны использовать средства вычислительной техники, которые не используются в личных целях и к которым применяются корпоративные меры по информационной безопасности.

1.2.12. В случае привлечения для сопровождения информационной инфраструктуры филиала субподрядной организации необходимо требовать от нее реализации мероприятий, предусмотренных пунктами 1.1-1.2.

2. Контроль за исполнением настоящего распоряжения оставляю за начальником отдела информационной безопасности М.С. Колбасом.

Врио директора  И.Ю. Хитринская

Лист ознакомления с распоряжением от «18» 08 2025 г. № 44:

С распоряжением ознакомлен(а): _____ Попов С.В. «___» _____ 2025 г.
подпись расшифровка подписи

С распоряжением ознакомлен(а): _____ Чойнзонов Е.Л. «___» _____ 2025 г.
подпись расшифровка подписи

С распоряжением ознакомлен(а): _____ Бессонова М.И. «___» _____ 2025 г.
подпись расшифровка подписи