Дата актуализации: 08.08.2025 г.

Технические требования к информационной и кибербезопасности при использовании ИТ-инфраструктуры Международного форума «Российская энергетическая неделя 2025» (ЦВЗ «Манеж», «Гостиный двор» г. Москва)

Санкт-Петербург, 2025

Оглавление

Требования к информационной безопасности на Мероприятии

В целях исключения различных видов угроз и минимизации рисков информационной безопасности (далее – ИБ) в период подготовки и проведения Международного форума «Российская энергетическая неделя 2025» (далее – Мероприятие) необходимо руководствоваться настоящими требованиями к информационной и кибербезопасности при использовании ИТ-инфраструктуры Мероприятия.

Особые условия и ограничения

1. В ИТ-инфраструктуре Мероприятия организована защита от несанкционированных подключений сторонних сетевых устройств – к одному порту сетевого оборудования может подключаться только одно устройство (один MAC-адрес).
2. Доступ из ИТ-инфраструктуры Мероприятия к некоторым ресурсам и сервисам сети Интернет может быть ограничен как до начала Мероприятия (во время монтажа), так и в процессе его проведения. Доступ может быть ограничен в том числе к стриминговым платформам, сервисам онлайн-трансляций и другим подобным сервисам.
3. На площадке проведения Мероприятия в постоянном режиме работает Штаб ИБ и функционирует Центр кибербезопасности, который в круглосуточном режиме осуществляет мониторинг и регистрацию событий информационной и кибербезопасности. В случае обнаружения инцидентов или выявления нарушений требований ИБ, которые могут привести к возникновению угроз безопасности и потенциальным деструктивным воздействиям ИТ-инфраструктуре Мероприятия, источник угрозы (персональный компьютер или сетевое устройство), а также предоставленный для его подключения сетевой порт, могут быть заблокированы (отключены) от ИТ-инфраструктуры до выяснения подробностей и устранения угрозы или нарушения.
4. В период подготовки и проведения Мероприятия заказчику/экспоненту необходимо определить ответственного за обеспечение ИБ ИТ-инфраструктуры стенда (застройки) и определить перечень применяемого оборудования на стенде.

Контакты ответственного от стенда и информацию об оборудовании стенда необходимо направить по форме, указанной в **Приложении № 1.**

Требования к ИТ-оборудованию, установленному на стенде

Для предотвращения несанкционированного доступа к компьютерному оборудованию стенда, где имеется техническая возможность, необходимо провести следующие работы:

1. Установить пароль на вход в операционную систему устройства.
2. Установить в настройках BIOS/UEFI загрузку только с системного жесткого диска или установить для загрузки системный жесткий диск первым в списке загрузки, установить пароль на вход в настройки BIOS/UEFI.
3. Установить средства антивирусной защиты (далее – СрАВЗ) из реестра отечественного ПО (reestr.digital.gov.ru/reestr) с актуальным набором антивирусных баз. Допускается использование СрАВЗ в предоставляемый разработчиком бесплатный пробный период.
4. Установить средство мониторинга обнаружения угроз ИБ. Программа для установки и необходимые инструкции будут направлены ответственному за обеспечение ИБ ИТ-инфраструктуры стенда (застройки).

Требования к используемому программному обеспечению

На используемых ИТ-устройствах стенда, подключенных к сети площадки проведения Мероприятия, необходимо установить актуальные версии операционной системы (далее – ОС) с последними обновлениями безопасности и актуальные версии программного обеспечения (далее – ПО) с последними стабильными обновлениями.

Для обеспечения соответствия требованиям рекомендуется использовать программное обеспечение, включенное в реестр отечественного ПО: reestr.digital.gov.ru/reestr.

К ПО **для удаленного администрирования** предъявляются следующие требования:

1. Во время подготовки к Мероприятию **до 14.10.2025 г.** разрешается использование ПО для удаленного администрирования из реестра отечественного ПО: reestr.digital.gov.ru/reestr. Например, программа удаленного управления «Ассистент»: мойассистент.рф. После указанной даты ПО для удаленного администрирования должно быть удалено с оборудования, подключаемого в сеть Мероприятия.
2. Для согласования использования ПО для удаленного администрирования во время проведения Мероприятия необходимо направить заявку согласно **Приложению № 2.**

Требования к сетевому оборудованию и организации внешнего управления

Для согласования организации внешнего управления на сетевом оборудовании стенда, включаемого в ИТ-инфраструктуру Мероприятия, необходимо направить заявку согласно **Приложению № 3.**

В случае отсутствия согласования или заявки внешнее управление оборудованием и доступ к нему из сети Интернет должны быть исключены.

При выявлении таких подключений устройство будет заблокировано.

Требования к организации VPN-подключений

Для согласования подключения устройств стенда к корпоративным VPN-сетям необходимо направить заявку согласно **Приложению № 4.**

В случае отсутствия согласования или заявки подключение устройств к VPN-сетям должно быть исключено.

При выявлении таких подключений устройство будет заблокировано.

Требования к организации вывода трансляций и презентационного контента на экранах, размещенных на площадке проведения Мероприятия

Для согласования вывода презентационного или видеоконтента из внешних источников (облачное хранилище, видеохостинг, веб-сайт и т. д.) необходимо направить заявку согласно **Приложению № 5.**

Запрещается вывод трансляций официальной программы Мероприятия из Интернета на экраны, установленные в павильонах и на стендах площадки проведения Мероприятия. Трансляция возможна исключительно посредством подключения к сети внутреннего инфовещания (ВТЗС).

Вывод любого контента с внешнего носителя на экраны, установленные в павильонах и на стендах, возможен только после антивирусной проверки носителя и контента.

Требования к организации видеоконференций

Для согласования организации видеоконференций, телемостов и других типов видеозвонков, организованных на стенде Мероприятия, необходимо направить заявку согласно **Приложению № 6.**

В случае отсутствия согласования или заявки трансляция использование ВКС-сеанса запрещено.

Общая информация

Заполненные заявки необходимо направить на адрес электронной почты: isecurity@roscongress.org.

В случае возникновения вопросов: ответственное лицо со стороны Организатора – **Торновский Константин Георгиевич, тел.: +7 (981) 699 1341.**

За нарушение требований информационной безопасности на участника (экспонента) будет наложен штраф в размере 200 000 (Двести тысяч) рублей за каждый выявленный факт нарушения в соответствии с договорными условиями.

Формы заявок для заполнения доступны на официальном сайте Мероприятия.

Приложение № 1

Форма для заполнения

Контакты ответственного за информационную безопасность стенда

Наименование Мероприятия:	
Наименование экспонента (заказчика стенда):	
Наименование стенда / локация на площадке:	
Подрядная организация, выполняющая работы:	
Контактное лицо по вопросам ИТ и информационной безопасности на период монтажа (ФИО, контактный телефон, эл. почта)	
Контактное лицо по вопросам ИТ и информационной безопасности на период Мероприятия (ФИО, контактный телефон, эл. почта)	
Дата заполнения:	

Информация об оборудовании стенда

№	Наименование оборудования	Используемая операционная система	Планируется подключение к сети Интернет (да/нет)	Оборудование используется для демонстрации контента (да/нет)
1.				
2.				

Должность *Подпись* *Ф. И. О.*

Тема письма:

«название мероприятия» год, РОС, «наименование юрлица», «название стенда»

Примечание:

1. Заполненную форму просим направлять на адрес isecurity@roscongress.org до **1 октября 2025 г.**

Приложение № 2

Форма для заполнения

Заявка на согласование удаленного администрирования

Наименование Мероприятия:		
Наименование экспонента (заказчика стенда):		
Наименование стенда:		
Подрядная организация, выполняющая работы:		
Контактное лицо:		
Телефон:		
Email:		
№	**Наименование**	**Информация**
1	IP-адрес управляемого оборудования	
2	Описание задач, требующих удаленного администрирования	
3	Используемое ПО для организации удаленного доступа	

Должность *Подпись* *Ф. И. О.*

Тема письма:

«название мероприятия» год, RA, «наименование юрлица», «название стенда»

Примечание:

1. Заполненную форму просим направлять на адрес isecurity@roscongress.org до **1 октября 2025 г.** Организатор не гарантирует рассмотрение заявок, поступивших после указанной даты.

Приложение № 3

Форма для заполнения

Заявка на согласование IP-адресов, используемых для внешнего управления

Наименование Мероприятия:		
Наименование экспонента (заказчика стенда):		
Наименование стенда:		
Подрядная организация, выполняющая работы:		
Контактное лицо:		
Телефон:		
Email:		
№	**Наименование**	**Информация**
1	Внешний IP-адрес	
2	IP-адрес управляемого оборудования	
3	Описание задач, требующих внешнего управления	
4	Используемое ПО (для организации VPN)	

Должность *Подпись* *Ф. И. О.*

Тема письма:

«название мероприятия» год, CTR, «наименование юрлица», «название стенда»

Примечание:

1. Заполненную форму просим направлять на адрес isecurity@roscongress.org до **1 октября 2025 г.** Организатор не гарантирует рассмотрение заявок, поступивших после указанной даты.

Приложение № 4

Форма для заполнения

Заявка на согласование VPN

Наименование Мероприятия:	
Наименование экспонента (заказчика стенда):	
Наименование стенда:	
Подрядная организация, выполняющая работы:	
Контактное лицо:	
Телефон:	
Email:	

№	Наименование	Информация
1	IP-адрес VPN-сервера	
2	IP-адрес VPN-клиента	
3	Описание задач, требующих внешнего управления	
4	Используемое ПО (для организации VPN)	

Должность *Подпись* *Ф. И. О.*

Тема письма:

«название мероприятия» год, VPN «наименование юрлица», «название стенда»

Примечание:

1. Заполненную форму просим направлять на адрес isecurity@roscongress.org до **1 октября 2025 г.** Организатор не гарантирует рассмотрение заявок, поступивших после указанной даты.

Приложение № 5

Форма для заполнения

Заявка на согласование внешних источников контента

Наименование Мероприятия:		
Наименование экспонента (заказчика стенда):		
Наименование стенда:		
Подрядная организация, выполняющая работы:		
Контактное лицо:		
Телефон:		
Email:		
№	**Наименование**	**Информация**
1	Перечень источников контента (ссылки, сеть вещания)	
2	Ф. И. О. и контактные данные представителя партнера/экспонента, ответственного за вывод контента	

Должность *Подпись* *Ф. И. О.*

Тема письма:

«название мероприятия» год, EXT, «наименование юрлица», «название стенда»

Примечание:

1. Заполненную форму просим направлять на адрес isecurity@roscongress.org до **1 октября 2025 г.** Организатор не гарантирует рассмотрение заявок, поступивших после указанной даты.

Приложение № 6

Форма для заполнения

Заявка на согласование использования видео-конференц-связи

Наименование Мероприятия:		
Наименование экспонента (заказчика стенда):		
Наименование стенда:		
Контактное лицо:		
Телефон:		
Email:		
№	**Наименование**	**Информация**
1	Дата и время использования ВКС	
2	Программное обеспечение для проведения ВКС	

Должность *Подпись* *Ф. И. О.*

Тема письма:

«название мероприятия» год, VCC, «наименование юрлица», «название стенда»

Примечание:

1. Заполненную форму просим направлять на адрес isecurity@roscongress.org до **1 октября 2025 г.** Организатор не гарантирует рассмотрение заявок, поступивших после указанной даты.