Федеральное государственное бюджетное образовательное учреждение высшего образования
"Сибирский государственный автомобильно-дорожный университет (СибАДИ)"

УТВЕРЖДЕНО
приказом П 22-471/ОД *от* 25.11.2022
Ректор ФГБОУ ВО «СибАДИ»
А.П. Жигадло
« 25 *»* ноября *2022 г.*

СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

Инструкция

по проведению антивирусного контроля

СМК И-УЦРиИТ- 2022

1. Общие положения

1.1. Настоящая инструкция по проведению антивирусного контроля (далее – инструкция) в Федеральном государственном бюджетном образовательном учреждении высшего образования «Сибирский государственный автомобильно-дорожный университет (СибАДИ)» (далее – университет, ФГБОУ ВО «СибАДИ») разработана с целью обеспечения защиты информации от угроз, исходящих от вредоносных и вирусных программ.

1.2. Инструкция разработана в соответствии с:

- Постановлением Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
- Приказом ФСТЭК РФ от 18 февраля 2013 г. N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

1.3. Инструкция предназначена для обязательного выполнения должностными лицами, осуществляющими антивирусный контроль, а так же для ознакомления всех пользователей персональных компьютеров (ПК) университета.

1.4. Инструкция вступает в силу с момента утверждения приказом ректора.

1.5. Все изменения и дополнения вносятся в инструкцию приказом ректора.

2. Осуществление антивирусной защиты

2.1. Антивирусная защита информации осуществляется на всех серверах и персональных компьютерах университета.

2.2. К применению на ПК допускается антивирусное средство, указанное в списке разрешенного программного обеспечения.

2.3. Установка и настройка антивирусных средств защиты осуществляется:

- системными администраторами (или программистами, исполняющими их обязанности) - на рабочих станциях и серверах;
- инженерами и техниками, осуществляющими сервисное обслуживание на рабочих станциях.

2.4. Антивирусный контроль должен осуществляться постоянно.

2.5. Периодическое обновление антивирусных баз должно осуществляться не реже одного раза в сутки.

2.6. Антивирусная проверка важных областей (проверка памяти ядра, загружаемых при запуске операционной системы объектов и загрузочных секторов) должна осуществляется автоматически после каждого обновления антивирусных баз.

2.7. При обнаружении компьютерного вируса пользователь ПК должен провести лечение или уничтожение зараженных файлов с использованием штатных антивирусных средств, затем повторно провести процедуру проверки (сканирования).

2.8. В случае обнаружения на компьютере или на съемном носителе информации, нового вируса, не поддающегося уничтожению или излечению, пользователь обязан прекратить какие-либо действия на ПК и незамедлительно поставить в известность системного администратора (или программиста, исполняющего его обязанности).

Сотрудник, выполняющий роль системного администратора обязан отключить ПК от компьютерной сети. При невозможности избавиться от вируса, сотрудник, выполняющий роль системного администратора, обязан доложить главному специалисту по комплексной защите информации об этом, для принятия совместного решения о дальнейших действиях.

Главный специалист по комплексной защите информации, должен инициировать служебное расследование с целью выявления источника зараженного файла.

Информация обо всех случаях обнаружения нового вируса и о принимаемых мерах немедленно доводится до начальника службы технической защиты информации Управления цифрового развития и информационных технологий (УЦРиИТ). Все дальнейшие действия выполняются в соответствии с его указаниями.

2.9. После удаления вируса, необходимо восстановить работоспособность операционной системы и прикладного программного обеспечения на ПК.

2.10. Пользователи ПК, перед началом работы со съемными носителями информации, обязаны проверить их на наличие (отсутствие) компьютерных вирусов.

2.11. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено системным администратором (или программистом, исполняющим его обязанности) на отсутствие вредоносных программ и компьютерных вирусов.

2.12. Запуск антивирусного программного средства должен осуществляться автоматически по заданию, централизованно созданному с использованием планировщика задач.

Если антивирус автоматически не загрузился, то необходимо незамедлительно сообщить об этом системному администратору.

2.15. Запрещается отключать антивирусное средство целиком или отдельные его функции, если это не входит в служебные обязанности сотрудника.

2.16. Для предотвращения проникновения вирусов в сеть университета, компьютеры, технические характеристики которых не соответствуют системным требованиям для установки антивирусного средства, должны быть отключены от компьютерной сети. На таких ПК запрещается использовать сменные носители информации.

Разработчик:
главный специалист по
комплексной защите информации Л.Е.Олейник 18.11.22

ЛИСТ СОГЛАСОВАНИЯ

Согласовано:

Проректор по НРиЦТ
«22» ноября 2022 г. _____ Корчагин П.А.

Начальник УЦРиИТ
«11» ноября 2022 г. _____ Чариков В.О.

Начальник ОКР
«22» 11 2022 г. _____ Бухарова М.Н.

Уполномоченный по
обеспечению СМК
«18» ноября 2022 г. _____ Стуцаренко И.А.

ЛИСТ ВНЕСЕНИЯ ИЗМЕНЕНИЙ

№ изменения	Дата распорядительного документа о внесении изменений, содержание изменения	Ф.И.О. и подпись лица, внёсшего изменения	Дата

ЛИСТ ОЗНАКОМЛЕНИЯ И СОГЛАСИЯ

№	Ф.И.О.	Должность	Подпись