Приложение № 5
к Приказу № 2132-О
от 01 декабря 2016 г.

Министерство образования и науки
Российской Федерации

Инструкция по антивирусной защите информационных систем персональных данных

В федеральном государственном бюджетном
образовательном учреждении
высшего образования
«Уфимский государственный
авиационный технический университет»

1. Общие положения

Настоящая инструкция определяет правила и основные требования по обеспечению антивирусной защиты и защиты от вредоносного программного обеспечения (далее - ПО) информационных систем персональных данных (далее - ИСПД), используемой в Федеральном государственном бюджетном учреждении высшего образования « Уфимский государственный авиационный технический университет» (далее – Университет), и устанавливает ответственность за их невыполнение.

Настоящая инструкция обязательна для выполнения всеми сотрудниками Университета.

2. Применение средств антивирусной защиты

2.1. Защита программного обеспечения ИСПД от вредоносного ПО осуществляется путем применения специализированных средств антивирусной защиты.

2.2. К использованию допускаются только лицензионные антивирусные средства, обладающие сертификатами регулирующих органов РФ.

2.3. Решение задач по установке и сопровождению средств антивирусной защиты возлагается на сотрудников управления информационных технологий

2.4 Частота обновления баз данных средств антивирусной защиты устанавливается не реже 1 раза в сутки.

2.5. Все впервые вводимое в эксплуатацию ПО должно проходить обязательный антивирусный контроль.

2.6. Контроль системы управления средствами антивирусной защиты осуществляется централизованно с рабочего места сотрудника управления информационных технологий

2.7. Средства антивирусной защиты устанавливаются на всех рабочих станциях и серверах Университета.

2.8. Еженедельно в установленное время в автоматическом режиме проводится антивирусный контроль всех дисков и файлов рабочих станций и серверов.

2.9. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, архивы), получаемая и передаваемая по телекоммуникационным каналам (включая электронную почту), а также информация на съемных носителях.

2.10. Контроль входящей информации необходимо проводить непосредственно после ее приема.

2.11. Контроль исходящей информации необходимо проводить непосредственно перед отправкой.

2.12. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

2.13. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь, обнаруживший проблему, должен провести внеочередной антивирусный контроль рабочей станции либо обратиться в управление информационных технологий.

2.14. При получении информации о возникновении вирусной эпидемии вне Университета должно быть осуществлено информирование пользователей о возможной эпидемии и рекомендуемых действиях.

2.15. В случае обнаружения зараженных компьютерными вирусами файлов пользователи обязаны:

- приостановить работу;
- провести лечение зараженных файлов;
- при невозможности вылечить зараженный файл поставить в известность управление информационных технологий;

2.16. Пользователям запрещается отключать, выгружать или деинсталлировать средства антивирусной защиты на рабочих станциях.

2.17. Настройка параметров средств антивирусной защиты осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.

2.18. Ответственный за безопасность ИСПД должен проводить расследования случаев появления вирусов для выявления причин и принятия соответствующих действий по их предотвращению.

2.19. Пользователи должны быть ознакомлены с данной инструкцией.