

УТВЕРЖДАЮ

Ректор ПГНИУ

_____/Макарихин И.Ю.

« ____ » _____ 20__ г.

ИНСТРУКЦИЯ

по антивирусной защите информационных систем

персональных данных ПГНИУ

1. Общие положения

Данный документ определяет правила и основные требования по обеспечению антивирусной защиты и защиты от вредоносного программного обеспечения (далее – ПО) информационных систем персональных данных (далее – ИСПД), используемых в ПГНИУ.

2. Инструкция по применению 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 уполномоченных органов РФ.
- 2.3 Решение задач по установке и сопровождению средств антивирусной защиты возлагается на администратора информационной безопасности ИСПД.
- 2.4 Частота обновления баз данных средств антивирусной защиты устанавливается не реже 1 раза в сутки.
- 2.5 Все впервые вводимое в эксплуатацию программное обеспечение должно проходить обязательный антивирусный контроль.
- 2.6 Контроль системы управления средствами антивирусной защиты осуществляется централизованно с рабочего места администратора ИСПД.
- 2.7 Средства антивирусной защиты устанавливаются на всех рабочих станциях и серверах ПГНИУ.
- 2.8 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.
- 2.9 Контроль входящей информации необходимо проводить непосредственно после ее приема.
- 2.10 Контроль исходящей информации необходимо проводить непосредственно перед отправкой.
- 2.11 Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.
- 2.12 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 к администратору ИСПД.
- 2.13 В случае обнаружения зараженных компьютерными вирусами файлов пользователи обязаны:
 - приостановить работу;
 - немедленно поставить в известность о факте обнаружения вируса администратора информационной безопасности ИСПД;
 - провести лечение зараженных файлов.
- 2.14 Пользователям запрещается отключать, выгружать или деинсталлировать средства антивирусной защиты на рабочих станциях.
- 2.15 Настройка параметров средств антивирусной защиты осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.