МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» (ФГБОУ ВО «ВГТУ», ВГТУ)

УТВЕРЖДАЮ
Ректор ВГТУ
_____ В.Р. Петренко
«_10_» _февраля_ 2016 г.

Система менеджмента качества

ИНСТРУКЦИЯ ПО АНТИВИРУСНОЙ ЗАЩИТЕ

Воронеж 2016

1 РАЗРАБОТАНА рабочей группой.

2 ОТВЕТСТВЕННЫЙ ИСПОЛНИТЕЛЬ начальник ОИСК Д.В. Макаров

3 УТВЕРЖДЕНА И ВВЕДЕНА В ДЕЙСТВИЕ приказом ректора ВГТУ
от 10.02.2016 № 05–01.18–0

4 ВВОДИТСЯ ВПЕРВЫЕ

1. Общие положения

1.1. Настоящая инструкция определяет порядок действий пользователей и администраторов информационной системы персональных данных (далее – ИСПДн) при применении средств антивирусной защиты.

1.2. Настоящая Инструкция разработана на основе следующих нормативных документов:

– Федеральный закон от 27.07.2006 № 149–ФЗ «Об информации, информационных технологиях и защите информации»;

– Федеральный закон от 27.07.2006 № 152–ФЗ «О персональных данных»;

– Приказ ФСТЭК России от 18.02.2013 года №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Постановление Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.3. Пользователи ИСПДн должны быть предупреждены об ответственности за невыполнение требований настоящей инструкции.

1.4. Пользователи ИСПДн должны быть ознакомлены с настоящей инструкцией до начала работы с ИСПДн под роспись.

1.5. Обязанность ознакомления сотрудников с настоящей инструкцией лежит на ответственном за организацию обработки ПДн.

2. Порядок организации антивирусной защиты

2.1. Программные средства антивирусной защиты являются частью системы защиты персональных данных ИСПДн.

2.2. Программные средства антивирусной защиты (далее – антивирусное ПО) устанавливается на средства вычислительной техники ИСПДн в соответствии с проектной документацией на систему защиты персональных данных ИСПДн.

2.3. Антивирусное ПО обеспечивает защиту от внедрения вредоносного программного обеспечения со съёмных носителей, через электронные отправления, из информационно-вычислительной сети, из сетей связи общего пользования и международного информационного обмена (Интернет).

2.4. Антивирусная защита ИСПДн строится как комплексная система, которая обеспечивает:

– управление конфигурацией и логической структурой всего программного обеспечения системы антивирусной защиты;

– управление установкой и обновлением лицензионных ключей средств антивирусной защиты;

– управление рассылкой и установкой обновлений баз средств антивирусной защиты;

– ограничение доступа пользователей на рабочих местах к настройкам установленных средств антивирусной защиты;

– настройку рассылки сообщений об обнаружении вирусов, о сбоях в работе средств антивирусной защиты и т.п.;

– решение проблем, возникающих в процессе использования средств антивирусной защиты.

2.5. При осуществлении антивирусной защиты ИСПДн выполняются следующие обязательные мероприятия:

– контроль съёмных носителей информации на предмет наличия на них вредоносного программного обеспечения до начала работы с ними;

– проверка всех электронных отправлений на предмет наличия вредоносного программного обеспечения;

– периодическая проверка на предмет наличия вредоносного программного обеспечения жёстких магнитных дисков (не реже одного раза в неделю);

– внеплановая проверка жёстких магнитных дисков и съёмных носителей информации в случае подозрения на наличие вредоносного программного обеспечения;

– восстановление работоспособности программных средств и информационных массивов, повреждённых программными вирусами.

2.6. Обновления баз данных средств антивирусной защиты в ИСПДн должно осуществляться в автоматическом режиме (не реже одного раза в сутки).

2.7. Установку и настройку антивирусного ПО осуществляет администратор безопасности в соответствии с эксплуатационной документацией на данное ПО.

3. Порядок действий при обнаружении вредоносного ПО

3.1. При обнаружении вредоносного программного обеспечения на съёмных носителях, в электронных отправлениях или при посещении ресурсов сети Интернет пользователь ИСПДн обязан:

– приостановить работу с источником угрозы (съёмным носителем, электронным отправлением, Интернет-ресурсом);

– сообщить администратору безопасности об обнаружении вредоносного программного обеспечения;

– принять меры по локализации и удалению вредоносного программного обеспечения, рекомендованные администратором безопасности.

3.2. При обнаружении вредоносного программного обеспечения в процессе обработки информации, за исключением п. 3.1, пользователь обязан:

– приостановить все работы на автоматизированном рабочем месте;

– сообщить администратору безопасности об обнаружении вредоносного программного обеспечения;

– принять меры по локализации и удалению вредоносного программного обеспечения, рекомендованные администратором безопасности.

3.3. При обнаружении вредоносного программного обеспечения на серверном или телекоммуникационном оборудовании, администратор безопасности обязан:

– немедленно сообщить ответственному за организацию обработки ПДн об обнаружении вредоносного программного обеспечения;

– принять меры по локализации и удалению вредоносного программного обеспечения, а также по выявлению источника и способа проникновения вредоносного программного обеспечения;

3.4. Администратор безопасности по факту событий по п.п. 3.1, 3.2, 3.3 должен зарегистрировать вирусную атаку в журнале событий безопасности в соответствии с Инструкцией по управлению событиями информационной безопасности.

3.5. В случае невозможности удаления вредоносного программного обеспечения, администратору безопасности следует обратиться в организацию, осуществляющую техническую поддержку средств антивирусной защиты. При передаче образцов заражённых файлов, а также при предоставлении информации о вирусной атаке в организацию, осуществляющую техническую поддержку средств антивирусной защиты информации, должны быть соблюдены требования конфиденциальности, обрабатываемой в ИСПДн информации.

3.6. После локализации и удаления вредоносного программного обеспечения в ИСПДн, администратор безопасности производит контроль целостности всех средств защиты информации, используемых в ИСПДн.