Приложение № 14 к приказу
от 28.06.2019 № 01-09/315
УТВЕРЖДЕНА
приказом генерального директора
КГБОУ ХКЦВР Созвездие
от 28.06.2019 № 01-09/315

ИНСТРУКЦИЯ

по организации антивирусной защиты

1. ВВЕДЕНИЕ

1.1. Настоящая инструкция определяет порядок организации антивирусной защиты и порядок действий администратора безопасности и пользователей при обнаружении вредоносного ПО.

2. ПОРЯДОК ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ

2.1. Программное обеспечение антивирусной защиты (далее – антивирус) устанавливают на все средства вычислительной техники. Антивирус обеспечивает защиту от внедрения вредоносного программного обеспечения со съемных носителей, через электронные отправления, из информационно-вычислительной сети, из сетей связи общего пользования и международного информационного обмена (Интернет).

2.2. Настройка антивирусной защиты обеспечивает:

2.2.1. Управление установкой и обновлением лицензионных ключей антивируса.

2.2.2. Установку обновлений антивируса.

2.2.3. Ограничение доступа пользователей на рабочих местах к настройкам антивируса.

2.2.4. Настройку рассылки сообщений об обнаружении вирусов, о сбоях и т.п.

2.3. На все средства антивирусной защиты должны быть документы, подтверждающие права на их использование.

2.4. При осуществлении антивирусной защиты выполняются следующие обязательные мероприятия:

2.4.1. Контроль съемных носителей информации на предмет наличия на них вредоносного программного обеспечения до начала работы с ними.

2.4.2. Проверка всех электронных отправлений на предмет наличия вредоносного программного обеспечения.

2.4.3. Периодическая проверка на предмет наличия вредоносного программного обеспечения жестких дисков (не реже одного раза в неделю).

2.4.4. Внеплановая проверка жестких дисков и съемных носителей информации в случае подозрения на наличие вредоносного программного обеспечения.

2.4.5. Восстановление работоспособности программных средств и информационных массивов, поврежденных программными вирусами.

2.5. Обновления баз данных средств антивирусной защиты осуществляется в автоматическом режиме.

2.6. Установку и настройку антивируса 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 съемных носителях, в электронных отправлениях или при посещении ресурсов сети Интернет пользователь обязан:

3.1.1. Приостановить работу с источником угрозы (съемным носителем, электронным отправлением, Интернет-ресурсом), иные работы на автоматизированном рабочем месте не запрещаются.

3.1.2. Сообщить администратору безопасности об обнаружении вредоносного программного обеспечения.

3.1.3. 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:

3.2.1. Приостановить все работы на автоматизированном рабочем месте.

3.2.2. Сообщить администратору безопасности об обнаружении вредоносного программного обеспечения.

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

3.4. В случае невозможности удаления вредоносного программного обеспечения, администратору безопасности следует обратиться в организацию, осуществляющую техническую поддержку средств антивирусной защиты. При передаче образцов зараженных файлов, а также при предоставлении информации о вирусной атаке в организацию, осуществляющую техническую поддержку средств антивирусной защиты

информации, должны быть соблюдены меры по обеспечению безопасности информации.

4. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

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

4.2. Пользователи должны быть ознакомлены с настоящей инструкцией под роспись. Обязанность ознакомления сотрудников с настоящей инструкцией лежит на администраторе безопасности.

4.3. Сотрудники несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей предусмотренных настоящей инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

5. НОРМАТИВНЫЕ И ПРАВОВЫЕ ДОКУМЕНТЫ

5.1. Приказ Федеральной службы по техническому и экспортному контролю Российской Федерации от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

5.2. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».