Приложение 3

К приказу ректора от 20.09.17 № 1063/01-01-04

Инструкция по антивирусному контролю

1. Общие положения

1.1 Настоящая инструкция разработана для работников ФГБОУ ВО «Удмуртский государственный университет» (далее – Университет) с целью регламентации правил антивирусного контроля, для поддержания высокого уровня защищенности от несанкционированного доступа, при обработке персональных данных (далее — ПД) с использованием средств автоматизации.

1.2 Настоящая инструкция определяет требования к организации антивирусного контроля в информационной системе от воздействий вредоносных программ и устанавливает обязанности и ответственность работников Университета в части антивирусной защиты ИСПД.

1.3 Выполнение требований настоящей инструкции является обязательным для всех работников Университета, участвующих в обработке ПД с применением средств автоматизации.

1.4 Для реализаций функций антивирусного контроля допускаются только лицензионные антивирусные средства, приобретенные у разработчиков или поставщиков данных средств.

1.5 Установка, настройка и сопровождение средств антивирусной защиты осуществляется ответственными лицами за осуществление антивирусного контроля в соответствии с требованиями разработчика данных средств.

Определения и принятые сокращения

Персональные данные (ПД) — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Информационная система персональных данных (ИСПД) — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Автоматизированное рабочее место (АРМ) — программно-технический комплекс автоматизированных средств, предназначенный для автоматизации деятельности определенного вида (ПК, ноутбук, терминал).

2. Классификация вредоносных программ

2.1 Вредоносные программы предназначены для получения несанкционированного доступа к информации, нарушая правила разграничения доступа.

2.2 Классификация вредоносных программ.

2.2.1 По вредоносным действиям:

- создание программно-аппаратных помех в работе АРМ и уничтожение данных;
- установка вредоносных программ (несанкционированная загрузка файлов, распаковка других вредоносных программ);
- кража, мошенничество, вымогательство, шпионаж за работниками (сканирование жесткого диска, регистрация нажатий клавиш, перенаправление на поддельные сайты, имитирующие исходные ресурсы, с целью получения атрибутов доступа работника к различным сервисам; блокирование доступа и вымогательство денежных средств);
- получение несанкционированного доступа к ресурсами АРМ или иным ресурсами, доступным через него с возможностью удаленного управления;
- использование АРМ без ведома работника, для проведения атак типа «отказ в обслуживании».
- использование АРМ без ведома работника, для рассылки коммерческой, политической и иной рекламы (спама).

2.2.2 По методу размножения:

- эксплойт (использование уязвимостей в программном обеспечении с целью захвата контроля над операционной системой или нарушения ее функциональности);
- логическая бомба (запуск при определенных временных или информационных условиях с целью несанкционированного доступа к информации или нарушения ее целостности);
- троянская программа (маскировка под легитимное программное обеспечение, компоненты и файлы данных с целью неумышленного запуска сотрудником и осуществления вредоносных действий);
- компьютерный вирус (внедрение в исполняемый код легитимного программного обеспечения или исполнительные команды (макросы): пакетные файлы Microsoft Word и Excel. Размножение происходит в пределах файлов и данных АРМ и через съемные носители;
- сетевой червь (распространение через локальные и глобальные компьютерные сети).

3. Признаки заражения АРМ вредоносной программой

3.1 Признаки заражения операционной системы:

- снижение работоспособности АРМ;
- аварийное завершение работы АРМ и периодические перезагрузки;
- некорректная работа установленных приложений;
- внезапная потеря файлов, данных и установленного программного обеспечения;
- отсутствие доступа к логическим или съемным дискам;
- всплывающие окна при запуске операционной системы;
- появление сообщений об ошибках;
- несанкционированное отключение средств антивирусного контроля;
- появление новых файлов, происхождение которых неизвестно;
- появление новых процессов в диспетчере задач, происхождение которых неизвестно;
- запрет или отсутствие возможности использования ранее доступных файлов, данных, функций и настроек операционной системы и прикладного программного обеспечения;
- появление нескольких несанкционированных копий файла (в некоторых случаях до полного заполнения свободного пространства на логических и съемных дисках);
- повышенная активность подключения к сетям международного обмена (Интернет), высокая и необоснованная плотность потока сетевого трафика;
- невозможность загрузки операционной системы из-за отсутствия ключевых системных файлов;
- периодические зависания операционной системы при загрузке ее компонентов;
- недоступность диспетчера задач операционной системы.

3.2 Признаки заражения сообщений электронной почты и средств передачи сообщений:

- получение сообщений от неизвестного адресата или сообщений от известного адресата с нехарактерным содержание или подозрительными вложениями.
- получение третьими лицами и адресатами в списке почтовых адресов сообщений от сотрудников сообщений с несанкционированными вложениями.
- рассылка рекламных сообщений с адреса работника.

4. Общие требования по антивирусному контролю

4.1 На каждом АРМ должно быть установлено и активировано лицензированное средство антивирусного контроля. Ответственность и контроль за исполнение данного пункта несет ответственное лицо за осуществление антивирусного конроля.

4.2 Установка средств антивирусного контроля (в том числе настройка параметров средств антивирусного контроля) на АРМ, серверах локальной вычислительной сети осуществляется администратором безопасности в соответствии с руководствами по применению данных антивирусных средств.

4.3 Приобретение средств вычислительной техники и программно-аппаратных продуктов должно осуществляться при непосредственном участии администратора безопасности.

4.4 Поступившие программно-аппаратные продукты должны быть подвергнуты входному контролю — проверке на отсутствие вредоносных программ и проверке длины контрольных сумм (если они указаны в сопроводительных документах).

4.5 Допуск работников Университета к АРМ осуществляется после ознакомления под подпись с настоящей инструкцией, инструкцией пользователя ИСПД и иными нормативными документами Университета в области обработки и защиты информации, а при необходимости — их обучения базовым навыкам работы с АРМ, установленным прикладным программным обеспечением и средствами антивирусного контроля.

4.6 Работникам Университета запрещается устанавливать и использовать стороннее программное обеспечение, не предусмотренные для исполнения своих служебных обязанностей или без согласования с администратором безопасности.

4.7 Работникам Университета при работе на АРМ в составе ИСПД запрещается несанкционированно подключать модемные и иные не предусмотренные устройства.

4.8 Работникам Университета запрещается открывать файлы, полученные из ненадежных источников без их предварительной проверки.

5. Применение средств антивирусного контроля

5.1 Настройка средств антивирусного контроля должна предусматривать периодическое обновление антивирусных баз.

5.2 Настройка средств антивирусного контроля должна предусматривать автоматический еженедельный плановый контроль файловой системы АРМ.

5.3 Внеочередной антивирусный контроль должен выполняться при обновлении или изменении программного обеспечения, а так же косвенных признаков заражения, указанных в разделе 2 настоящей инструкции.

5.4 В случае обнаружения косвенных признаков заражения АРМ, указанных в разделе 2 настоящей инструкции или в случае обнаружения вредоносных программ и зараженных файлов по результатам антивирусной проверки работники обязаны:

- отключить АРМ от сети международного информационного обмена (Интернет) и локальной сети;
- прекратить работу на АРМ, закрыть все приложения;

- поставить в известность о факте обнаружения вредоносных программ и зараженных файлов ответственных лиц;
- провести с помощью средств антивирусной защиты проверку жестких и съемных носителей, вылечить или удалить зараженный файл (при необходимости привлечь администратора безопасности).

5.5 Настройка средств антивирусного контроля должна предусматривать автоматическое ведение журнала событий о фактах обнаружения вредоносных программ, зараженных файлах и предпринятых действий и их результатов по нейтрализации данных угроз.

5.6 Работники Университета обязаны с помощью средств антивирусного контроля проводить проверку любых загружаемых и входящих файлов, а так же информации на съемных носителях, при их подключении к АРМ.

6. Ответственность

6.1 Ответственность за поддержание установленного в настоящей инструкции порядка проведения антивирусного контроля возлагается на администратора безопасности.

6.2 Работники Университета несут предусмотренную законодательством РФ ответственность, за невыполнение задач и функций, возложенных на них настоящей инструкцией.