Приложение № 3
к Приказу №2132-О
от 01 декабря 2016 г.

Министерство образования и науки
Российской Федерации

Инструкция пользователя информационной системы персональных данных

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

1. Общие положения

Настоящая Инструкция устанавливает обязанности пользователя информационной системы персональных данных (далее - ИСПД) в Федеральном государственном бюджетном учреждении высшего образования «Уфимский государственный авиационный технический университет» (далее – Университет) по обеспечению безопасности обрабатываемых в ней персональных данных, запреты на действия пользователя в ИСПД, а также его права и ответственность.

Доступ пользователя к ИСПД осуществляется в соответствии с перечнем сотрудников, допущенных к обработке персональных данных.

Доступ пользователя к автоматизированному рабочему месту (далее -АРМ) назначаются в соответствии с правами доступа в ИСПД.

Контроль за выполнением настоящей Инструкции возлагается на ответственного за защиту информации в подразделении.

Каждый работник Университета, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным (в дальнейшем именуемый пользователь), несёт персональную ответственность за свои действия при работе с информационными ресурсами ИСПД.

2.Обязанности пользователя ИСПД

Пользователь обязан:

2.1. При работе с документами, содержащими персональные данные, руководствоваться требованиями документации ИСПД. Строго соблюдать установленные правила обеспечения безопасности персональных данных при работе с программными и техническими средствами ИСПД.

2.2. Использовать ИСПД для выполнения служебных задач в соответствии с должностной инструкцией.

2.3. Использовать для доступа к ИСПД собственную уникальную учетную запись (логин) и пароль.

2.4. Хранить в тайне пароли и PIN-коды, обеспечивать физическую сохранность ключевого носителя доступа к ИСПД.

2.5. Не допускать при работе с ИСПД просмотр посторонними лицами персональных данных, отображаемых на дисплее АРМ или иных носителях.

2.6. Блокировать экран дисплея АРМ парольной заставкой при оставлении рабочего места.

2.7. По всем вопросам, связанным с обеспечением защиты персональных данных, содержащихся в базах данных, и работе со средствами защиты информации, возникающими при работе в ИСПД, обращаться к ответственному за безопасность ИСПД.

2.8. Немедленно прекращать обработку персональных данных и ставить в известность ответственного за безопасность ИСПД при подозрении компрометации пароля, а также при обнаружении:

- нарушений целостности пломб, наклеек на персональные электронно-вычислительные машины при наличии таковых, или иных фактов совершения в его отсутствие попыток несанкционированного доступа;
- несанкционированных изменений в конфигурации программных или аппаратных средств АРМ;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования АРМ;
- непредусмотренных конфигурацией АРМ отводов кабелей и подключенных устройств.

2.9.Немедленно информировать ответственного за безопасность ИСПД в случае обнаружения попыток несанкционированного доступа к ИСПД.

2.10. Немедленно информировать сотрудников, осуществляющих сетевое администрирование, при появлении сообщений от программного обеспечения антивирусной защиты о возможном вирусном заражении АРМ или возникновении неисправностей (сбоев) в работе сервисов и информационных ресурсов Университета.

3. Действия, запрещенные пользователю ИСПД

Пользователю ИСПД запрещается:

3.1. Предоставлять доступ к информации, содержащей персональные данные, лицам, не допущенным к их обработке.

3.2. Записывать пароль на любые носители, в том числе бумажные.

3.3.Сообщать (или передавать) посторонним лицам личные ключи или атрибуты доступа к ресурсам ИСПД.

3.4. Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования соответственным за безопасность ИСПД.

3.5.Копировать информацию, содержащую ПД на узлы сети, не входящие в ИСПД.

3.6.Выводить на печать информацию, содержащую персональные данные на принтеры, печать на которых не согласована с ответственным за безопасность ИСПД.

3.7. Осуществлять доступ к ИСПД с узлов сети, не назначенных ответственным за безопасность в качестве АРМ ИСПД.

3.8. Самостоятельно изменять конфигурацию аппаратно-программных средств в ИСПД.

3.9. Осуществлять действия по преодолению установленных ограничений на доступ к ИСПД.

3.10.Отключать или изменять конфигурацию средств защиты информации ИСПД.

3.11. Устанавливать на АРМ программное обеспечение, несвязанное с исполнением служебных обязанностей.

4. Права пользователя ИСПД

Пользователь ИСПД имеет право:

4.1. Получать помощь по вопросам эксплуатации ИСПД от ответственного за безопасность ИСПД.

4.2. Обращаться к сотрудникам, осуществляющим сетевое администрирование, по вопросам дооснащения АРМ техническими и программными средствами, не входящими в штатную конфигурацию АРМ и ИСПД, необходимыми для автоматизации деятельности в соответствии с возложенными на него должностными обязанностями.

4.3. Подавать сотрудникам, осуществляющим сетевое администрирование, предложения по совершенствованию функционирования ИСПД.

5.Ответственность пользователя ИСПД

Пользователь ИСПД несет ответственность за:

5.1. Обеспечение безопасности персональных данных при их обработке в ИСПД.

5.2. Нарушение работоспособности или вывод из строя системы защиты ИСПД.

5.3. Преднамеренные действия, повлекшие модификацию или уничтожение персональных данных ИСПД, и несанкционированный доступ к персональным данным в ИСПД.

5.4. Разглашение персональных данных.

5.5. Пользователь, имеющий расширенные права «Опытный пользователь» или «Администратор», несет ответственность за корректное функционирование прикладного программного обеспечения ИСПД.

5.6. За нарушение настоящей Инструкции к пользователю могут применяться меры дисциплинарного воздействия.

6.Правила работы в информационно-телекоммуникационных сетях международного информационного обмена

6.1. Работа в информационно-телекоммуникационных сетях международного информационного обмена-сети Интернет и других (далее - Сеть) на элементах ИСПД должна проводиться только при служебной необходимости.

6.2. При работе в Сети запрещается:

– осуществлять работу при отключенных средствах защиты (антивирусных, межсетевых экранов и других);

– передавать по Сети защищаемую информацию;

– скачивать из Сети программное обеспечение и другие файлы в неслужебных целях;

– посещать сайты сомнительной репутации (сайты, содержащие нелегально распространяемое программное обеспечение, сайты знакомств, онлайн игры и другие).