Приложение № 3
к приказу
от 09.06.2023 № 444-П

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в СГТУ имени Гагарина Ю.А.

1. Общие положения

Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в СГТУ имени Гагарина Ю.А. (далее – Правила) разработаны в соответствии с требованиями, установленными Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», локальными нормативными актами СГТУ имени Гагарина Ю.А. (далее – Университет) и устанавливают порядок проведения мероприятий, направленных на выявление и устранение нарушений, а также определение соответствия обработки и защиты персональных данных в Университете Конституции Российской Федерации, Трудовому кодексу Российской Федерации, Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных», постановлению Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлению Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», приказу ФСТЭК от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», приказу ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», локально-нормативным актам Университета в сфере обработки и защиты персональных данных.

2. Основание для проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

2.1. Основанием для проведения внутреннего контроля за соответствием обработки и защиты персональных данных в Университете требованиям законодательства, локально-нормативных актов Университета (далее – внутреннего контроля) является разработанный и утвержденный на учебный год, ректором Университета или лицом, исполняющим его обязанности, План проведения внутреннего контроля за соответствием обработки и защиты персональных данных в Университете.

3. Состав комиссии внутреннего контроля

3.1. Комиссия внутреннего контроля (далее – Комиссия) формируется из членов Комиссии по вопросам обработки и защиты персональных данных в Университете и иных работников Университета и утверждается приказом ректора Университета или лицом, исполняющим его обязанности.

3.2. Комиссия должна состоять не менее чем из 3 человек, включая руководителя Комиссии, эксперта и технического эксперта.

3.3. Руководитель Комиссии выполняет следующие функции:

– распределение ответственности между членами Комиссии;

– проведение совещания в начале осуществления внутреннего контроля;

– осуществление контроля;

– согласование подготовленных отчетов;

– подготовка и согласование итогового отчетного документа по результатам проведения внутреннего контроля.

3.4. Технический эксперт, включенный в состав Комиссии, выполняет следующие функции:

– осуществление подготовки проведения внутреннего контроля;

– проведение анализа документов по направлению внутреннего контроля;

– формирование отчета по внутреннему контролю;

– участие в подготовке итогового отчетного документа по внутреннему контролю.

3.5. В качестве технического эксперта, включенного в состав Комиссии, выступает работник управления информатизации и телекоммуникаций Университета.

3.6. Технический эксперт оказывает содействие в формировании выводов внутреннего контроля.

3.7. В случае необходимости дополнительно привлекаются в состав Комиссии другие технические эксперты.

4. Принципы проведения внутреннего контроля

4.1. Проведение внутреннего контроля не должно нарушать рабочий процесс в структурных подразделениях Университета.

4.2. Комиссия должна соблюдать требования конфиденциальности при работе со сведениями и документами, получаемыми и составляемыми в ходе внутреннего контроля.

4.3. Комиссия и все получатели отчета внутреннего контроля должны обеспечивать его конфиденциальность.

5. Программа проведения внутреннего контроля

5.1. При проведении внутреннего контроля Комиссия проверяет:

5.1.1. наличие в положении о структурном подразделении и должностных инструкциях обязанностей и ответственности работников, в части обработки и защиты персональных данных;

5.1.2. наличие отметки о прохождении работниками, осуществляющими обработку персональных данных, инструктажа по обеспечению конфиденциальности при обращении с информацией, содержащей персональные данные, с Политикой обработки персональных данных СГТУ имени Гагарина Ю.А., Положением об обработке и защите персональных данных СГТУ имени Гагарина Ю.А., Инструкцией об обеспечении конфиденциальности при обращении с информацией, содержащей персональные данные в СГТУ имени Гагарина Ю.А;

5.1.3. наличие перечня должностей работников структурного подразделения, выполняющих обработку персональных данных;

5.1.4. организацию учета используемых в структурном подразделении съемных носителей информации, применяемых для обработки и хранения персональных данных;

5.1.5. наличие условий хранения материальных носителей персональных данных (допускается только в помещениях или шкафах, оборудованных надежными замками и другими необходимыми средствами защиты от несанкционированного проникновения);

5.1.6. организацию раздельного хранения материальных носителей персональных данных, обработка которых осуществляется в различных целях;

5.1.7. использование при обработке персональных данных учтенных средств вычислительной техники (далее – СВТ) (не допускается использование личных и неучтенных в установленном порядке СВТ);

5.1.8. корректную работу СВТ, применяемую для обработки персональных данных (отсутствие проблем функционирования программного и аппаратного обеспечения);

5.1.9. возможные факты подключения неучтенных технических устройств и носителей информации, а также внесение изменений в

программную среду СВТ, применяемых для обработки персональных данных;

5.1.10. наличие и состояние антивирусной защиты (корректная работа, наличие последних на дату проверки обновлений антивирусного программного обеспечения и баз данных сигнатур вирусов);

5.1.11. наличие и состояние средств защиты информации;

5.1.12. наличие полученных в установленном порядке прав и атрибутов (логин, пароль) доступа к информационным системам персональных данных (далее – ИСПД), доменным учетным записям;

5.1.13. выполнение работником правил работы с атрибутами доступа (не передавать другим лицам, исключить возможность просмотра, не хранить на бумажных или электронных носителях в открытом (незашифрованном) виде);

5.1.14. факты нарушения установленного порядка передачи атрибутов доступа учетных записей;

5.1.15. возможные факты нарушения установленного порядка выноса материальных носителей информации, содержащих персональные данные, за пределы Университета;

5.1.16. возможные факты передачи персональных данных по телефону, факсу и другим незащищенным каналам связи, а также диктовке персональных данных вслух.

5.2. В случае вступления изменений законодательства в области персональных данных в период проведения проверки необходимо обратить внимание на проведение мероприятий по приведению обработки и защиты персональных данных в соответствие с ними.

6. Оформление результатов внутреннего контроля

6.1. Результаты проведения внутреннего контроля структурного подразделения оформляются экспертом в виде отчета и акта о выявленных нарушениях.

6.2. По завершении проведения в соответствии с утвержденным планом внутреннего контроля структурных подразделений, оформляется итоговый отчетный документ и акт о выявленных нарушениях, который составляется руководителем Комиссии путем объединения отчетов экспертов.

6.3. Итоговый отчетный документ должен содержать:

– оценку текущего состояния правовых, организационных, инженерно-технических (технических и программных) мероприятий по обеспечению защиты персональных данных при их обработке и хранении;

– оценку существующего порядка и принятых мер по обеспечению защиты персональных данных при их обработке и хранении;

– оценку того, выполняются или не выполняются соответствующие требования по обеспечению защиты персональных данных при их обработке и хранении (в итоговой отчетной документации должны быть отражены все свидетельства (доказательства) внутреннего контроля);

– общие выводы относительно соответствия реального уровня защищенности персональных данных при обработке и хранении допустимому уровню риска;

– рекомендации по проведению комплекса согласованных мер правового, технического и организационно-технического характера, направленных на выявление и ликвидацию различных видов угроз и организацию эффективно функционирующей системы защиты персональных данных при их обработке;

– рекомендации по разработке аналитического обоснования создания (модернизации) системы (подсистемы) защиты персональных данных при их обработке в Университете.