МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Система менеджмента качества

ИНСТРУКЦИЯ
ПО КОНТРОЛЮ (АНАЛИЗУ) ЗАЩИЩЁННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

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 администратора безопасности и системных администраторов информационной системы при проведении контроля (анализа) защищённости персональных данных при их обработке в информационной системе персональных данных (далее – ИСПДн).

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. Администратор безопасности и администраторы системные ИСПДн должны быть предупреждены об ответственности за действия, нарушающие требования настоящей инструкции.

1.4. Администратор безопасности и системные администраторы ИСПДн должны быть ознакомлены с настоящей инструкцией до начала работы с ИСПДн под роспись. Обязанность ознакомления администратора безопасности и системных администраторов ИСПДн с настоящей инструкцией лежит на ответственном за организацию обработки ПДн.

2. Порядок контроля защищённости персональных данных

2.1. Контроль защищённости персональных данных проводится с целью контроля и оценки фактического состояния защищённости персональных данных при их обработке в ИСПДн.

2.2. Контроль защищённости проводится на плановой основе, а в случае необходимости – внепланово.

2.3. Периодичность плановых процедур выявления, анализа и устранения уязвимостей ИСПДн составляет 1 год.

2.4. Внеплановые процедуры контроля защищённости проводят по распоряжению ответственного за организацию обработки ПДн в случае необходимости.

2.5. Необходимость внеплановой процедуры определяет ответственный за организацию обработки персональных данных на основе анализа **журнала событий безопасности**.

2.6. Контроль защищённости персональных данных включает:

- выявление, анализ уязвимостей ИСПДн;
- контроль установки обновлений программного обеспечения ИСПДн;
- контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации;
- контроль составе технических средств, программного обеспечения и средств защиты информации;
- другие проверки.

3. Выявление, анализ и устранение уязвимостей

3.1. В ИСПДн должно осуществляться выявление и устранение следующих типов уязвимостей:

- недостатки и (или) ошибки программного обеспечения ИСПДн и её системы защиты информации;
- недостатки аппаратных средств ИСПДн, в том числе аппаратных средств защиты информации;
- организационно-технические недостатки.

3.2. Мероприятия по выявлению, анализу и устранению уязвимостей организует ответственный за организацию обработки ПДн. Непосредственными исполнителями мероприятий по выявлению, анализу и устранению уязвимостей ИСПДн являются администратор безопасности и системные администраторы ИСПДн.

4. Выявление, анализ и устранение недостатков программного обеспечения

4.1. Проверка конфигурации и настроек программно – технических средств ИСПДн и системы защиты персональных данных на соответствие требованиям эксплуатационной документации на систему защиты персональных данных ИСПДн и требований к защите персональных данных.

4.2. Проверка наличия и сроков действия лицензий на установленное программное обеспечение, в том числе программное обеспечение средств защиты информации.

4.3. Проверка установки последних обновлений используемого программного обеспечения, в том числе программное обеспечение средств защиты информации:

– проверка установки критических обновлений безопасности на используемое в ИСПДн программное обеспечение;

– проверка соответствия установленных версий программного обеспечения актуальным версиям, рекомендованным разработчиком;

– проверка обновлений баз данных средств антивирусной защиты;

– проверка обновлений баз решающих правил для средств обнаружения вторжений (при использовании средств обнаружения вторжений);

– проверка обновлений баз признаков уязвимостей.

4.4. Анализ сообщений об уязвимостях из специальных источников.

4.5. Результаты проверок по п.4.1, 4.2, 4.3 и 4.4 администратор безопасности оформляет в виде **Акта проверки программных средств** (приложение 1**).**

4.6. Устранение обнаруженных недостатков на основании своих полномочий осуществляют администратор безопасности и системные администраторы ИСПДн.

4.7. При наличии в ИСПДн программных сканеров безопасности, администратор безопасности осуществляет процесс сканирования и анализ отчётов об обнаруженных уязвимостях.

4.8. Результаты сканирования должны быть отсортированы администратором безопасности по степени критичности (опасности реализации известных угроз безопасности) обнаруженных уязвимостей и представлены в виде акта о **результатах сетевого сканирования** (приложение 2).

5. Выявление, анализ и устранение недостатков аппаратных средств

5.1. К недостаткам аппаратных средств, используемых в ИСПДн, относят низкую надёжность функционирования (частые аппаратные сбои, отключения), нарушения аппаратной конфигурации, низкое качество контактных соединений.

5.2. При выявлении недостатков аппаратных средств проверяют:

– техническое состояние аппаратных средств, журналы планово-профилактического обслуживания аппаратных средств ИСПДн за период контроля защищённости ИСПДн;

– наличие сертификатов соответствия на применяемые в ИСПДн и её системе защиты информации аппаратные средства;

– наличие у поставщиков обновлённых версий аппаратных средств, применяемых в ИСПДн, а также в составе системы защиты ИСПДн;

– перечень событий информационной безопасности за период контроля, связанных с отказами и неисправностями аппаратных средств;

– конфигурацию соединений и установки аппаратных средств, условия их эксплуатации.

5.3. Проверку осуществляет администратор безопасности и оформляет её результаты в виде Акта **проверки аппаратных средств** (приложение 3).

5.4. Обнаруженные в ходе проверки отклонения от конфигурации ИСПДн устраняет администратор безопасности и системные администраторы, каждый в своей части. Координирует работы администратор безопасности.

5.5. При обнаружении аппаратных средств с низкой надёжностью, частыми выходами из строя администратор безопасности принимает меры по ремонту или замене этих аппаратных средств.

6. Выявление, анализ и устранение организационно-технических недостатков

6.1. Проверка состояния и актуальности организационно-распорядительной документации (далее – ОРД) по защите персональных данных, обрабатываемых в ИСПДн.

6.2. Проверка заполнения рабочих документов ОРД (записи в журналах, перечнях, актах и других формах по требованиям ОРД).

6.3. Проверка соответствия выполнения правил генерации и смены паролей пользователей принятым требованиям.

6.4. Проверка соответствия выполнения правил заведения и удаления учётных записей пользователей принятым требованиям.

6.5. Проверка соответствия выполнения правил разграничения доступа к персональным данным и ресурсам ИСПДн принятым требованиям.

6.6. Проверка соответствия полномочий пользователей принятым требованиям.

6.7. Проверка наличия документов, подтверждающих правомерность изменений учётных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей.

6.8. Проверка состояния физической защиты ИСПДн (средства охраны и физического доступа в контролируемой зоне ИСПДн).

6.9. Проверка знания и соблюдения пользователями ИСПДн основных нормативно-правовых актов в области защиты информации и требований ОРД.

6.10. Проверки организует ответственный за организацию обработки ПДн с участием администратора безопасности.

6.11. **Результаты проверки организационно – технических мер защиты** оформляются в соответствии с приложением 4.

Приложение 1

Форма акта проверки программных средств

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

УТВЕРЖДАЮ

_____
должность

_____
ФИО

« ___ » _____ 20___ г.

АКТ №_____
проверки программных средств

Настоящий акт составлен администратором безопасности о том, что проведена проверка программных средств

Программное обеспечение	Содержание проверки	Обнаруженные уязвимости/недостатки	Рекомендации

Администратор безопасности

« ___ » _____ 20___ г. _____ _____
подпись *ФИО*

Приложение 2

Форма акта о результатах сетевого сканирования

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

УТВЕРЖДАЮ

_____

должность

_____

ФИО

« ___ » _____ 20___ г.

АКТ №_____
о результатах сетевого сканирования

Настоящий акт составлен администратором безопасности о том, что проведено сетевое сканирование

Уязвимость	IP адрес/имя	Описание угрозы	Рекомендации
Высокий риск			
Средний риск			

Администратор безопасности

« ___ » _____ 20___ г. _____ _____

подпись *ФИО*

Приложение 3

Форма акта проверки аппаратных средств

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

УТВЕРЖДАЮ

_____

должность

_____

ФИО

« ___ » _____ 20___ г.

АКТ №_____
проверки аппаратных средств

Настоящий акт составлен администратором безопасности о том, что проведена проверка аппаратных средств:

Оборудование	Содержание проверки	Обнаруженные уязвимости/недостатки	Рекомендации

Администратор безопасности

« ___ » _____ 20___ г. _____ _____

подпись *ФИО*

Приложение 4

Форма акта проверки организационно-технических мер по защите персональных данных

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

УТВЕРЖДАЮ

_____

должность

_____

ФИО

« ___ » _____ 20___ г.

АКТ №_____

проверки организационно-технических мер по защите персональных данных

Настоящий акт составлен администратором безопасности о том, что проведена проверка организационно-технических мер по защите персональных данных

Объект проверки	Содержание проверки	Обнаруженные уязвимости/недостатки	Рекомендации

Администратор безопасности

« ___ » _____ 20___ г. _____ _____

подпись *ФИО*