П-141/2019

Министерство образования и науки Самарской области
ГБПОУ «ТК им. Н.Д. Кузнецова»

Протокол заседания Совета Учреждения
от 29.10.2019г. № 20

Протокол заседания Совета обучающихся
Учреждения
от 29.10.2019г. № 20

Протокол заседания Совета родителей
Учреждения
от 29.10.2019г. № 20

УТВЕРЖДАЮ
Директор
ГБПОУ «ТК им. Н.Д. Кузнецова»
_____А.Н. Сакеев
«29» октября 2019г.

Приказ № 522 о/д от 29.10.2019

Инструкция
по контролю защищенности персональных данных

1. Введение

1.1. Настоящая инструкция определяет порядок действий администратора безопасности и администраторов системных информационной системы при контроле защищенности персональных данных, обрабатываемых в ИСПДн.

2. Выявление, анализ и устранение уязвимостей.

2.1. Уязвимость – это недостаток ИСПДн или системы защиты информации, который может привести к реализации угрозы безопасности ПДн, обрабатываемых в ИСПДн.

2.2. Периодичность плановых процедур выявления, анализа и устранения уязвимостей ИСПДн составляет 1 год. Внеплановые процедуры выявления, анализа и устранения уязвимостей ИСПДн проводят по распоряжению ответственного за организацию обработки ПДн в случае необходимости. Необходимость внеплановой процедуры выявления и устранения уязвимостей определяет ответственный по организации обработки ПДн на основе анализа журналов событий безопасности.

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

2.3.1. Недостатки и (или) ошибки программного обеспечения ИСПДн и ее системы защиты информации;

2.3.2. Недостатки аппаратных средств ИСПДн, в том числе аппаратных средств защиты информации;

2.3.3. Организационно-технические недостатки.

2.4. 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 администраторы системные ИСПДн.

3. Выявление, анализ и устранение недостатков программного обеспечения.

3.1. Проверка конфигурации и настроек программно – технических средств ИСПДн и системы защиты информации на соответствие требованиям эксплуатационной документации и требований к защите информации.

3.2. Проверка наличия и сроков действия лицензий на установленное программное обеспечение.

3.3. Проверка наличия последних обновлений используемого программного обеспечения:

3.3.1. проверка соответствия обновлений версиям программного обеспечения, установленного в ИСПДн и системе защиты информации;

3.3.2. проверка обновлений вирусных баз;

3.3.3. проверка обновлений баз решающих правил для средств обнаружения вторжений (при использовании средств обнаружения вторжений).

3.3.4. Проверка обновлений баз признаков уязвимостей.

3.4. Анализ сообщений об уязвимостях из специальных источников.

3.5. Результаты проверок по п.3.1, 3.2, 3.3 и 3.4 администратор безопасности оформляет в виде таблицы результатов проверки программных средств по форме, принятой в Организации.

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

3.7. При наличии в ИСПДн сканеров безопасности, администратор безопасности осуществляет процесс сканирования и анализ отчетов об обнаруженных уязвимостях.

3.8. Результаты сканирования должны быть отсортированы администратором безопасности по степени критичности (опасности реализации известных угроз безопасности) обнаруженных уязвимостей и сведены в таблицу результатов сетевого сканирования по форме , принятой в Организации.

4. Выявление, анализ и устранение недостатков аппаратных средств.

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

4.2. При выявлении недостатков аппаратных средств проверяют:

4.2.1. техническое состояние аппаратных средств, журналы планово-профилактического обслуживания аппаратных средств ИСПДн за период контроля защищенности ИСПДн;

4.2.2. наличие сертификатов соответствия на примененные в ИСПДн и ее системе защиты информации аппаратные средства;

4.2.3. наличие у поставщиков обновленных версий аппаратных средств, примененных в ИСПДн и системе защиты информации;

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

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

4.3. Проверку осуществляет администратор безопасности и оформляет ее результаты в таблицу результатов проверки аппаратных средств по форме, принятой в Организации.

4.4. Обнаруженные в ходе проверки отклонения от конфигурации ИСПДн устраняет администратор безопасности и администраторы системные , каждый в своей части. Координирует работы администратор безопасности. При обнаружении аппаратных средств с низкой надежностью, частыми выходами из строя администратор безопасности принимает меры по ремонту или замене этих аппаратных средств.

5. Выявление, анализ и устранение организационно-технических недостатков.

5.1. Проверка состояния и актуальности организационно-распорядительной документации (далее ОРД) по защите информации, обрабатываемой в ИСПДн.

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

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

5.4. Проверка соответствия выполнения правил заведения и удаления учетных записей пользователей принятым требованиям.

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

5.6. Проверка соответствия полномочий пользователей принятым требованиям.

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

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

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

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

5.11. Результаты проверки организационно – технических мер защиты оформляются в виде таблицы по форме, принятой в Организации.

6. Заключительные положения

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

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

7. Нормативные и правовые документы.

7.1. 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 РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Разработчик:
заместителя директора по общим вопросам

_____/ Ю.Ю. Алексеев /

Лист
ознакомления с «Инструкцией по контролю защищенности персональных данных»

№ п/п	ФИО	Должность	Подпись, дата