Экзамен по дисциплине «Организация защиты информации»

Состоит из 1 практического задания и 2 вопросов.

Практическое задание.

В организации имеется основная информационная система.

Информационная система внедрена сторонней организацией на основе договорных отношений с использованием системы управления базами данных PostgreSQL. База данных размещается на собственном серверном оборудовании с использованием средств виртуализации.

Информационная система функционирует на базе общей инфраструктуры организации в качестве прикладного сервиса по клиент-серверной технологии и доступна на 50 компьютерах. Все компьютеры информационной системы имеют подключение к вычислительной сети организации.

В организации имеется контроллер домена, рабочие станции находятся под управлением операционных систем семейства Windows (Windows 7, Windows 8.1, Windows 10).

Каждый компьютер закреплен за конкретным сотрудником организации. Режим обработки информации в информационной системе многопользовательский с разграничением прав доступа пользователей на уровне Active Directory и СУБД (у каждого сотрудника персональная учетная запись). Для доступа к операционной системе и СУБД сотрудниками используются пароли.

Обновление применяемых операционных систем и прикладного программного обеспечения осуществляется не систематически.

На каждом компьютере установлено актуальное средство антивирусной зашиты.

Сотрудники имеют возможность подключать личные внешние машинные носители информации к компьютерам.

Все технические средства информационной системы размещены в рамках одного здания в соседних помещениях. В здании организован контрольно-пропускной режим.

Инфраструктура организации имеет централизованное подключение к сети «Интернет», организуемое оператором связи на основе договорных отношений. К вычислительной сети организации подключены точки доступа Wi-Fi, для доступа сотрудников, в том числе с использованием личных устройств, к сети «Интернет». Подключение к точке доступа осуществляется с использованием пароля.

В информационной системе не применяются технологии автоматизации управления технологическим процессом, облачные технологии, технологии больших данных, суперкомпьютеры, грид-вычисления, кластеризация.

Управление (администрирование) информационной системой, а также обслуживание ее технических и программных средств осуществляется

собственным специалистом с привлечением на основе договорных отношений компании, внедрившей информационную систему.

Обработка защищаемой информации осуществляется в информационной системе, а также в офисном прикладном программном обеспечении. Защищаемая информация хранится централизовано в базе данных, а также в файлах локально на компьютерах.

Для информационной системы необходимо определить:

1. Категории информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, которая должна обрабатываться в информационной системе, исходя из специфики организации;
2. Класс защищенности информационной системы если бы она имела статус государственной информационной системы;
3. Негативные последствия, которые могут наступить от реализации (возникновения) угроз безопасности информации;
4. Виды, категории и возможности нарушителей безопасности информации.

В ответе должны содержаться результаты проделанной работы с ходом определения (логическое рассуждение) каждого из 4 значений.

В качестве рассматриваемой организации каждый студент на экзамене получает по одной организацию из разных сфер деятельности.

Первый вопрос из перечня:

1. Понятие персональных данных.
2. Понятие оператора персональных данных.
3. Категории персональных данных.
4. Специальные категории персональных данных.
5. Понятие биометрических персональных данных.
6. Понятие персональных данных, разрешенных субъектом персональных данных для распространения.
7. Иные категории персональных данных.
8. Конфиденциальность персональных данных.
9. Общедоступные источники персональных данных.
10. Понятие обработки персональных данных.
11. Виды обработки персональных данных.
12. Понятие автоматизированной обработки персональных данных.
13. Виды согласий на обработку персональных данных.
14. Первый принцип обработки персональных данных.
15. Второй принцип обработки персональных данных.
16. Третий принцип обработки персональных данных.
17. Четвертый принцип обработки персональных данных.
18. Пятый принцип обработки персональных данных.
19. Шестой принцип обработки персональных данных.
20. Седьмой принцип обработки персональных данных.
21. Первое условие обработки персональных данных.
22. Первое условие обработки специальных категорий персональных данных.
23. Первое условие обработки биометрических персональных данных.
24. Поручение на обработку персональных данных.
25. Понятие информационной системы персональных данных.

Второй вопрос из перечня:

1. Понятие системы защиты информации. Группы мер защиты информации. Привести примеры правовых, организационных и технических мер защиты информации.
2. Меры защиты информации по идентификации и аутентификации субъектов доступа и объектов доступа с примерами.
3. Меры защиты информации по управлению доступом субъектов доступа к объектам доступа с примерами.
4. Меры защиты информации по ограничению программной среды с примерами.
5. Меры защиты информации по защите машинных носителей информации с примерами.
6. Меры защиты информации по регистрации событий безопасности с примерами.
7. Меры защиты информации по антивирусной защите с примерами.
8. Меры защиты информации по обнаружению (предотвращению) вторжений с примерами.
9. Меры защиты информации по контролю (анализу) защищенности информации с примерами.
10. Меры защиты информации по обеспечению целостности информационной системы и информации с примерами.
11. Меры защиты информации по обеспечению доступности информации с примерами.
12. Меры защиты информации по защите среды виртуализации с примерами.
13. Меры защиты информации по защите технических средств с примерами.
14. Меры защиты информации по защите информационной системы, ее средств, систем связи и передачи данных с примерами.

В качестве мер защиты информации достаточно привести 3-4 меры из соответствующей группы в соответствии с Требованиями, утвержденными приказом ФСТЭК России от 11.02.2013 № 17.