УТВЕРЖДАЮ
Директор
_____ К.В.Багмет
Приложение №7 к приказу №26
от «29» апреля 2019 года

ПОЛИТИКА
аудита информационной безопасности
ГАУ ДПО «Центр повышения квалификации и профессиональной переподготовки работников социальной сферы»

1. Общие положения

Данный документ устанавливает требования и процедуры аудита информационной безопасности.

Целями проведения аудита ИБ информационных систем являются:

1) оценка соответствия ГАУ ДПО Центр повышения квалификации и профессиональной переподготовки работников социальной сферы (далее – Центр ДПО) требованиям нормативных документов, относящимся к деятельности Центра ДПО;

2) обеспечение достаточной уверенности в том, что СОИБ, включая защитные меры, функционирует надлежащим образом и адекватна существующим угрозам ИБ;

3) определение способов повышения эффективности СОИБ.

Различают внешний и внутренний аудит. Внешний аудит должен проводится сторонней компанией, не участвующей в эксплуатации СОИБ не реже раз в 3 года. Внутренний аудит ИБ Центра ДПО проводиться лицами, не участвующими в тех же процессах реализации СОИБ и представляет собой непрерывную деятельность.

Задачами проведения аудита информационной безопасности являются:

1) анализ рисков ИБ Центра ДПО;

2) оценка текущего уровня защищенности информационных ресурсов;

3) оценка соответствия СИБ существующим требованиям законодательства РФ в области информационной безопасности;

4) оценка выполнения требований внутренних документов Центра ДПО в части ИБ;

5) выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов СИБ.

Этапы аудита информационной безопасности включают в себя ряд последовательных этапов:

1) инициирование процедуры аудита ИБ;

2) проведение аудита ИБ;

3) анализ данных аудита ИБ;

4) выработка рекомендаций по результатам проведенного аудита ИБ;

5) подготовка аудиторского отчета по результатам проведенного аудита ИБ.

2. Инициирование процедуры аудита ИБ

Аудит ИБ проводится по инициативе директора Центра ДПО.

Аудитором должен быть подготовлен и согласован проект Приказа о проведении аудита ИБ, включающий в себя План проведения аудита ИБ и состав комиссии по аудиту.

Приказ о проведении аудита ИБ утверждается директором Центра ДПО.

В состав комиссии по аудиту ИБ должны входить:

1) представитель руководства Центра ДПО, курирующий вопросы информационной безопасности;

2) ответственный за информационную безопасность.

На этапе инициирования процедуры аудита в Плане по аудиту ИБ указываются следующие границы проведения обследования:

1) список проверяемых структурных подразделений Центра ДПО;

2) список обследуемых физических, программных и информационных ресурсов;

3) площадки (помещения), попадающие в границы обследования;

4) основные виды угроз ИБ, рассматриваемые при проведении аудита ИБ;

5) список проверяемых организационно-распорядительных и методических документов по ИБ Центра ДПО.

3. Сбор и анализ данных аудита ИБ

Получение информации о Центре ДПО, его организационной структуре, пользователях ИС и структурных подразделениях, функционировании и текущем состоянии ИС осуществляется аудитором в ходе интервью с ответственными лицами Центра ДПО, путем изучения технической организационно-распорядительных и методических документов по ИБ Центра ДПО, а также исследования ИС и рабочих мест с использованием специализированного программного инструментария.

Выводы относительно положения дел в Центре ДПО с информационной безопасностью делаются аудитором после анализа всех необходимых исходных данных.

Все работники обязаны оказывать содействие аудиторам и предоставлять всю необходимую для проведения аудита информацию.

4. Рекомендации по итогам аудита ИБ

Рекомендации, выдаваемые аудитором по результатам анализа состояния ИС, определяются используемым подходом, особенностями

обследуемой ИС, состоянием информационной безопасностью и степенью детализации, используемой при проведении аудита ИБ.

Организационные меры защиты имеют приоритет над программно-техническими мерами защиты.

5. Подготовка аудиторского отчёта

Аудиторский отчёт является основным результатом проведения аудита ИБ.

Структура отчёта может существенно различаться в зависимости от характера и целей проводимого аудита.

Определены обязательные разделы аудиторского отчёта:

1) Термины и определения;
2) Общие положения;
3) План аудита ИБ;
4) Мероприятия аудита ИБ;
5) Выводы по итогам аудита ИБ;
6) Рекомендации по устранению выявленных нарушений;
7) Рекомендации по улучшению СИБ.