# КИБЕРБЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ ИНФОРМАЦИОННЫХ СЕТЕЙ

**Цель программы —** углубленное практическое изучение вопросов сетевой компьютерной безопасности, построения и эксплуатации защищенных информационных систем.

**Выпускники курса получают свидетельство о повышении квалификации в области технической защиты информации государственного образца.**

**Целевая аудитория:**

- руководители подразделений технической защиты информации, информационной безопасности, ответственные за состояние информационной безопасности и организацию работ по созданию в организациях комплексных систем защиты информации;
- аналитики по вопросам компьютерной безопасности, ответственные за анализ состояния информационной безопасности;
- специалисты, ответственные за разработку необходимых нормативно-методических и организационно-распорядительных документов по вопросам защиты информации.

**Требуемая предварительная подготовка слушателей:**

- общие представления об информационных системах, правовых, организационных и технических аспектах обеспечения информационной безопасности компьютерных систем;
- базовые знания по IP-сетям, основным протоколам и службам стека TCP/IP;
- навыки работы с ОС Windows NT или Linux.

**Форма обучения –** очная (дневная).
**Стоимость обучения одного слушателя** – 1700 рублей.

Обучение проводится по адресу: г. Минск, ул. К. Цеткин, 24, 11 этаж в соответствии с графиком учебного процесса.

Продолжительность программы – 58 академических часов.

**Учебный план курса**

| № п/п | Название тем курса |
|---|---|
| | **Основы обеспечения безопасности информации. Государственное регулирование деятельности в сфере защиты информации** |
| 1. | Информационная безопасность, защита информации, кибербезопасность. Методология обеспечения безопасности информации |
| 2. | Государственное регулирование деятельности в сфере защиты информации |
| 3. | Концепция информационной безопасности |
| 4. | Требования по обеспечению технической и криптографической защиты информации в системах, обрабатывающих информацию, распространение и предоставление которой ограничено, в том числе на КВОИ |
| 5. | Особенности и порядок отнесения объектов информации к КВОИ |
| 6. | Анализ рисков информационных систем, количественные и качественные значения рисков. Формирование плана обработки риска |
| 7. | Уязвимости и эксплойты |
| | **Методы и средства обеспечения безопасности информации** |
| 8. | Криптографические средства защиты информации |
| 9. | Электронные документы и электронная цифровая подпись |
| 10. | Технические средства защиты информации. Проблемы безопасности беспроводных сетей и интернета вещей |
| 11. | Прикладные протоколы. Описание и применение прикладных протоколов |
| 12. | Прикладные протоколы. DHCP. DNS. HTTP. SMTP. HTTPS. Установка и настройка серверов для работы по прикладным протоколам |
| 13. | Мониторинг сетевых устройств. SNMP и NetFlow. Системы мониторинга. Сбор и анализ диагностических сообщений: syslog, snmp |
| | **Правовое регулирование защиты персональных данных** |
| 14. | Правовое регулирование защиты персональных данных |

| | |
|---|---|
| 15. | **Функциональная безопасность информационных систем** |
| 16. | Безопасность технологий виртуализации и облачных вычислений |
| 17. | Безопасность уровня операционных систем |
| | **Тренды киберпреступности. Социотехнические кибератаки в информационных системах** |
| 18. | Тренды киберпреступности. Социотехнические кибератаки в информационных системах |