Практическое применение технологий информационной безопасности + КИБЕРУЧЕНИЯ (advance)

Цель программы — сформировать у слушателей комплексное понимание и практические навыки владения методами компьютерной безопасности при работе по выявлению, реагированию и расследованию киберинцидентов.

Выпускники курса получают свидетельство о повышении квалификации в области кибербезопасности государственного образца.

Целевая аудитория:

- руководители структурных подразделений центров обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций;
- специалисты центров обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций;
- линейные сотрудники служб информационной безопасности;
- специалисты, обеспечивающие кибербезопасность.

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 в ОС Windows или Linux.

Форма обучения – очная (дневная).
Стоимость обучения одного слушателя – 3500 рублей.

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

Продолжительность программы – 50 академических часов.

Учебный план курса

№ п/п	Название тем курса
I	**Методология расследования инцидентов.**
1.	Кибербезопасность, информационная безопасность, защита информации. Опыт противодействия киберберпреступности (на примере Республики Беларусь и Российской Федерации)
2.	Типовая корпоративная информационная система.
3.	Продвинутые кибератаки. Матрица MITRE ATT&CK. Модель Cyber Kill Chain. Индикаторы компрометации.
4.	Жизненный цикл информационной безопасности.
II	**Active Directory**
1.	Домены Active Directory. Доменная групповая политика.
2.	Работа с групповыми политиками AD.
3.	Доменная аутентификация. Типовые атаки на протоколы аутентификации**.**
4.	Типовые атаки на AD.
III	**Введение в LDAP.**
1.	Введение в LDAP.

2.	Безопасность в LDAP. Мониторинг и отладка LDAP. Резервное копирование и восстановление данных LDAP.
3.	Установка и настройка сервера LDAP.
4.	Модели данных LDAP.
5.	Интеграция с другими сервисами.
6.	Восстановление LDAP.
7.	Отладка и защита LDAP.
IV	**Восстановление систем**
1.	Использование восстановления после сдерживания угроз.
2.	Применение защитных мер при атаке на инфраструктуру.
3.	Восстановление сервисов после сдерживания угроз.
4.	Методология расследования инцидентов ИБ в SIEM. Типовые Use Cases.
V	**Киберучения.**
1.	Отработка сценария «атака вируса-шифровальщика» на киберполигоне. Анализ результатов, обсуждение и разбор сценария.
2.	Настройка защитных мер в инфраструктуре.
3.	Отработка сценария «атака скриптами» на киберполигоне. Проверка реализованной системы защиты с восстановлением доступности инфраструктуры. Анализ результатов, работа над ошибками. Разбор атак.