АННОТАЦИЯ
к дополнительной профессиональной программе

Вид программы: повышения квалификации

Название ДПП: «Виктимологический анализ и профилактика киберпреступлений в деятельности полиции»

Категория обучающихся: специалисты с высшим образованием и средним профессиональным образованием.

Цель: формирование и развитие у сотрудников полиции профессиональных компетенций, знаний и практических навыков, необходимых для эффективного предупреждения киберпреступлений путем воздействия на их потенциальных и реальных жертв.

Задачи:

- изучение кибервиктимности: анализ механизмов и факторов (поведенческих, психологических, цифровых), которые делают граждан или организации уязвимыми для киберпреступников (например, при дистанционном мошенничестве или социальной инженерии).
- освоение методов виктимологического анализа: обучение составлению «портрета жертвы», выявлению групп риска в цифровой среде и прогнозированию виктимного поведения.
- разработку мер превентивного воздействия: освоение тактики индивидуальной и общей профилактики, направленной на повышение цифровой грамотности населения, снижение виктимного потенциала граждан и активизацию их защитных свойств в интернете.
- совершенствование деятельности ОВД: оптимизация межведомственного взаимодействия и внедрение современных форм защиты прав потерпевших от преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.

По окончании освоения ДПП обучающийся должен:

Знать:

- основные методы и приемы регуляции актуального состояния и восстановления функционального состояния при работе с жертвами киберпреступлений;
-виктимогенные детерминанты, способствующие совершению IT-преступлений
- основные методы и приемы оказания психологической помощи в особых условиях;

Уметь:

- проводить виктимологический мониторинг для оценки оперативной обстановки;
- выявлять и классифицировать потенциальные жертвы и уязвимые группы населения, наиболее подверженные рискам цифровой виктимизации;
-разрабатывать и реализовывать превентивные меры и программы по снижению уровня виктимности граждан в сфере ИТТ;
-анализировать особые условия деятельности;
-прогнозировать и организовывать правовое просвещение населения и формировать цифровую культуру безопасности.

Практический опыт:

- владеть навыками применения методик виктимологического анализа для оценки рисков совершения киберпреступлений на обслуживаемой полицией территории;
- владеть технологиями проведения индивидуальной профилактической работы с лицами, обладающими повышенной виктимностью
-владеть алгоритмами взаимодействия органов правопорядка с другими государственными структурами, общественными организациями и ИТ-компаниями при осуществлении совместных программ кибербезопасности;

Формы итоговой аттестации: тестовый контроль, практическое задание.