



Негосударственное образовательное учреждение  
дополнительного профессионального образования  
«ЦЕНТР ПРЕДПРИНИМАТЕЛЬСКИХ РИСКОВ»



**Программа повышения квалификации**

**«Повышение эффективности системы  
безопасности предприятия на основе  
применения видеоаналитики»**

г. Санкт-Петербург  
2015 год

Программа обсуждена и одобрена на заседании учебно-методического совета  
НОУ ДПО «ЦПР»  
Протокол №23 от 25 июня 2015 года.

Секретарь  М.В.Бочков

Дополнительная профессиональная образовательная программа повышения квалификации «**Повышение эффективности системы безопасности предприятия на основе применения видеоаналитики**» (далее – Программа) разработана авторским коллективом НОУ ДПО «ЦПР» в соответствии с Федеральным законом Российской Федерации от 29.12.2012 г. № 273-ФЗ "Об образовании в Российской Федерации"; Приказом Минобрнауки РФ № 499 от 1 июля 2013 г. «Об утверждении порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам». При разработке содержания настоящей дополнительной профессиональной образовательной Программы учтены требования обеспечения преемственности по отношению к федеральным государственным образовательным стандартам высшего образования (ФГОС ВПО) по направлению подготовки "Информационная безопасность", а также имеющиеся на момент формирования Программы требования профессиональных стандартов и (или) квалификационные требования, указанные в квалификационных справочниках, утверждаемых в порядке, устанавливаемом Правительством Российской Федерации, по соответствующим должностям, профессиям, специальностям (в соответствии с Общероссийским классификатором специальностей).

## **СОДЕРЖАНИЕ**

<b>1.ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ</b>	<b>4</b>
1.1. Цель Программы	4
1.2. Характеристика подготовки по Программе	5
1.3. Требования к уровню подготовки слушателя	5
1.4. Требования к результатам освоения Программы	6
<b>2. СОДЕРЖАНИЕ ПРОГРАММЫ</b>	<b>9</b>
2.1. Учебный план	9
2.2. Содержание Программы	11
<b>3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ</b>	<b>12</b>
3.1. Требования к минимальному материально-техническому обеспечению	12
3.2. Информационное обеспечение обучения	13
Перечень рекомендуемой литературы, Интернет-ресурсов	
<b>4. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ</b>	<b>16</b>
Примерные вопросы для подготовки к зачету	

## 1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

### 1.1. Цель Программы

Программа предназначена для повышения квалификации:

- руководителей, начальников отделов и специалистов подразделений безопасности;
- специалистов по ИТСО и САЗ, имеющих опыт работы в обеспечении физической безопасности объектов предприятия;
- инженеров, специалистов отделов ИТ, прикладных программистов, обеспечивающих разработку, модернизацию и сопровождение ИТСО и других средств защиты объектов;
- руководителей и сотрудников служб охраны, караулов, специализированных технических отделов и служб по обеспечению сохранности людских, материальных и информационных ресурсов.

Целью реализации Программы является совершенствование профессиональных компетенций, повышение профессионального уровня обучающихся в рамках имеющейся квалификации в условиях изменения целей, содержания, технологий, нормативно-правового обеспечения профессиональной деятельности в сфере информационной безопасности.

Программа проводится в форме профессионального тренинга и предназначена для подготовки руководителей и специалистов к решению задач анализа, наращиваемой в системах контроля и управления доступом, системах видеонаблюдения и других автоматизированных системах предприятия видеоинформации.

В ходе практических занятий рассматриваются примеры решения задач видеоаналитики на основе существующего и перспективного оборудования защиты объектов, и применения специального программного обеспечения. Повышение эффективности систем безопасности обеспечивается возможностью оперативного выявления индикаторов риска, оперативного реагирования и расследования событий безопасности.

Учебная Программа «Повышение эффективности системы безопасности предприятия на основе применения видеоаналитики» рекомендована в качестве вариативного раздела (модуля) программы профессиональной переподготовки «Комплексное обеспечение безопасности предприятия» со специализацией «Организация защиты объектов предприятия инженерно-техническими средствами охраны».

Специфика Программы заключается в ее прагматической направленности. Программа повышения квалификации призвана ликвидировать разрыв между требуемыми актуальными и существующими компетенциями слушателей, который не может быть преодолен средствами самообразования и самоподготовки на рабочем месте. Этот факт определяет требования к конечным результатам обучения по Программе: формирование

профессиональных компетенций работника, позволяющие ему выполнять свои трудовые функции в рамках актуальных требований к его профессиональной деятельности.

Программа характеризуется практической ориентированностью обучения, с опорой на имеющийся у слушателей трудовой опыт, высокую долю самостоятельной работы, прикладной характер содержания образования.

## **1.2. Характеристика подготовки по Программе**

Нормативный срок освоения Программы – 40 академических часов, 5 рабочих дней, включая все виды аудиторной и внеаудиторной (самостоятельной) учебной работы слушателя.

Режим обучения: 40 ак.часов аудиторных занятий в неделю (8 ак.часов в день) - лекции, семинары, практические занятия.

Форма обучения – очная, с отрывом от производства.

## **1.3. Требования к уровню подготовки слушателя**

Повышение квалификации по настоящей Программе осуществляется на базе высшего и среднего профессионального образования.

К освоению данной дополнительной профессиональной Программы допускаются лица имеющие среднее профессиональное и (или) высшее образование.

Для успешного освоения Программы повышения квалификации обучающийся должен:

### **1. Знать и понимать:**

- место и роль информационной безопасности в системе национальной безопасности Российской Федерации;
- основные нормативные правовые акты в области информационной безопасности и защиты информации;
- правовые основы организации защиты информации,
- принципы и методы организационной защиты информации;

### **2. Уметь:**

- анализировать и оценивать угрозы информационной безопасности объекта;
- пользоваться нормативными документами по защите информации;
- использовать в практической деятельности правовые знания; анализировать основные правовые акты и осуществлять правовую оценку информации, используемой в профессиональной деятельности.

### **3. Владеть:**

- навыками работы с нормативными правовыми актами в сфере экономической и информационной безопасности;

- навыками компьютерной обработки служебной документации, статистической информации и деловой графики; работы с информационно-поисковыми и информационно-справочными системами и базами данных, используемыми профессиональной деятельностью;
- навыками организации и обеспечения режима секретности;
- навыками обоснования, выбора, реализации и контроля результатов управленческого решения.

#### **1.4. Требования к результатам освоения Программы**

Программа направлена на совершенствование и (или) освоение следующих профессиональных компетенций:

- способность понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах (ПК-1);
- способность использовать нормативные правовые документы в своей профессиональной деятельности (ПК-2);
- способность формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности (ПК-3);
- способность организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации (ПК-4);
- способность организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов (ПК-5);
- способность определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия (ПК-6);
- способность проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов (ПК-7);
- способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью (ПК-8);
- способность формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью (ПК-9);
- способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых

- программно-аппаратных, криптографических и технических средств защиты информации (ПК-10);
- способность изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации (ПК-11);
- способность участвовать в работах по реализации политики информационной безопасности (ПК-12);
- способность применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности (ПК-13);
- способность организовать работу малого коллектива исполнителей с учетом требований защиты информации (ПК-14);
- способность организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю (ПК-15).

В результате освоения Программы слушатель должен приобрести и (или) усовершенствовать следующие знания и умения, необходимые для качественного изменения компетенций:

- выявление потенциальных и реальных угроз информационной безопасности; умение проводить их ранжирование по вероятности реализации и величине ущерба;
- осуществление организационно-правового обеспечения информационной безопасности объекта защиты;
- организация работы малых коллективов исполнителей с учетом требований защиты информации;
- совершенствование системы управления информационной безопасностью;
- изучение и обобщение опыта работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации;
- контроль эффективности реализации политики информационной безопасности объекта.
- участие в проведении аттестации объектов, помещений, технических средств, систем, программ и алгоритмов на предмет соответствия требованиям защиты информации;
- знание методов и средств выявления угроз безопасности автоматизированным системам;
- знание методов технической защиты информации;
- знание методов формирования требований по защите информации;
- знание методов организации и управления деятельностью служб защиты информации на предприятии;
- знание методик проверки защищенности объектов информатизации на соответствие требованиям нормативных документов;
- изучение технических каналов утечки информации, возможностей

технических разведок, способов и средств защиты информации от утечки по техническим каналам, методов и средств контроля эффективности технической защиты информации;

- изучение принципов и методов противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;
- изучение принципов организации информационных систем в соответствии с требованиями по защите информации.



## 2. СОДЕРЖАНИЕ ПРОГРАММЫ

### 2.1. Учебный план

**Учебный план**  
программы повышения квалификации  
**«Повышение эффективности системы безопасности предприятия на  
основе применения видеоаналитики»**

**Цель:** подготовка специалиста к организации антитеррористической защиты предприятия, основам правового использования ИТСО и САЗ, основам анализа уязвимости системы физической защиты предприятия.

**Категория слушателей:** руководители, начальники отделов и специалисты подразделений безопасности; специалисты по ИТСО и САЗ, имеющих опыт работы в обеспечении физической безопасности объектов предприятия; инженеры, специалисты отделов ИТ, прикладные программисты, обеспечивающие разработку, модернизацию и сопровождение ИТСО и других средств защиты объектов; руководители и сотрудники служб охраны, караулов, специализированных технических отделов и служб по обеспечению сохранности людских, материальных и информационных ресурсов.

**Срок освоения:** 40 часов, 5 учебных дней

**Режим занятий:** 8 часов в день

№ п/п	Наименование учебных тем	Количество часов на курс подготовки			
		Всего	в том числе:		
Лекции, семинары	Практические занятия		Формы контроля		
1	Видеонаблюдение, как базовый механизм обеспечения информационно-аналитической работы подразделения безопасности	6	6		
2	IP-сети, как телекоммуникационная инфраструктура систем видеонаблюдения.	8	2	6	
3	Подходы к применению видеоаналитики при построении систем защиты объектов на предприятиях ТЭК	10	6	4	
4	Применение видеоаналитики при решении задач оценки достоверности информации, полученной при проведении собеседований и опросов	10	4	6	
5	Актуальные проблемы применения	4	4		

	<b>видеонаблюдения и видеоналитики в системе безопасности предприятия</b>				
	<b>Итоговая аттестация</b>	<b>2</b>		<b>2</b>	<b>Зачет без оценки</b>
	<b>Итого</b>	<b>40</b>	<b>22</b>	<b>18</b>	

## 2.2. Содержание Программы

### Учебная программа повышения квалификации «Повышение эффективности системы безопасности предприятия на основе применения видеоаналитики»

#### Тема 1. Видеонаблюдение, как базовый механизм обеспечения информационно-аналитической работы подразделения безопасности.

Место и роль видеонаблюдения в системе обеспечения безопасности предприятия. Видеоаналитика как перспективное направление повышения эффективности системы безопасности предприятия. Основы правового использования видеонаблюдения и видеоизображений людей в деятельности подразделения безопасности предприятий ТЭК.

#### Тема 2. IP-сети, как телекоммуникационная инфраструктура систем видеонаблюдения.

Возможности современного оборудования IP-сетей. Реализация функций видеоаналитики в современных системах видеонаблюдения. Практикум: Особенности формирования, передачи и хранения видеoinформации в IP-сетях. Практикум: Применение современных IP-камер для реализации функций видеоаналитики. Возможности открытого программного обеспечения по реализации функций видеоаналитики по реализации видеоаналитических функций. Практикум. Возможности современного программного обеспечения по аналитической работе с архивами видеoinформации.

#### Тема 3. Подходы к применению видеоаналитики при построении систем защиты объектов на предприятиях ТЭК.

Общие и отраслевые решения внедренческих компаний по применению систем видеоаналитики на объектах ТЭК. Технические средства построения систем видеонаблюдения и регламентация их применения на объектах ТЭК. Интеграция систем видеонаблюдения с другими подсистемами безопасности предприятия.

#### Тема 4. Применение видеоаналитики при решении задач оценки достоверности информации, полученной при проведении собеседований и опросов.

Методика подготовки и анализа видеoinформации при расследовании нарушений корпоративной политики безопасности, в том числе содержащих признаки противоправных действий и преступлений. Практикум: Возможности современного программного обеспечения по обработке и анализу видеoinформации. Совместный анализ данных видеонаблюдения и записей электронных журналов в среде аналитических программ.

#### Тема 5. Актуальные проблемы применения видеонаблюдения и видеоаналитики в системе безопасности предприятия.

### **3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ**

Обучение проводится на учебно-методической базе Негосударственного образовательного учреждения дополнительного профессионального образования «Центр предпринимательских рисков».

К преподаванию учебной Программы привлекаются преподаватели, имеющие большой опыт педагогической деятельности (более 5 лет) в сфере экономической безопасности и практический опыт работы по этой тематике.

В процессе обучения применяются современные технические средства обучения и методические пособия, разработанные по темам учебной Программы.

#### **3.1. Требования к минимальному материально-техническому обеспечению**

Реализация Программы дисциплины требует наличия учебного кабинета с необходимыми техническими средствами обучения.

##### **Оборудование учебного кабинета:**

- рабочие места по количеству обучающихся (стол, стул, необходимые для работы в аудитории канцелярские принадлежности);
- рабочее место преподавателя (стол, стул, необходимые для работы в аудитории канцелярские принадлежности);
- доска для записей с принадлежностями (маркеры для письма, указка).

##### **Технические средства обучения:**

- персональный компьютер преподавателя с периферийными устройствами и доступом к сети Интернет;
- мультимедиа-проектор с экраном;
- персональные компьютеры (ноутбуки) по количеству обучающихся с доступом к сети Интернет.

Каждый обучающийся обеспечивается раздаточным материалом и компакт-дискон с записью учебно-методических материалов Программы (презентации преподавателей, конспекты, нормативно-правовые акты, образцы рассматриваемых на занятиях документов, примеры решения практических задач, статьи и другие материалы по темам Программы).

## 3.2. Информационное обеспечение обучения

### Перечень рекомендуемой литературы, Интернет-ресурсов

#### Законы и нормативные акты

Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (действующая редакция)

«Доктрина информационной безопасности Российской Федерации» (утв. Президентом РФ 09.09.2000 N Пр-1895) (действующая редакция)

Федеральный закон от 28.12.2010 N 390-ФЗ (ред. от 05.10.2015) «О безопасности» (действующая редакция)

Закон РФ «О государственной тайне» от 21.07.1993г. №5485-1 (действующая редакция)

Федеральный закон «О коммерческой тайне» от 29 июля 2004 г. N 98-ФЗ (действующая редакция)

Федеральный закон «О персональных данных» от 27 июля 2006 г. N 152-ФЗ (действующая редакция)

Федеральный закон «Об электронной подписи» от 6 апреля 2011 г. N 63-ФЗ (действующая редакция)

Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (Зарегистрировано в Минюсте России 14.05.2013 N 28375) (действующая редакция)

#### Учебная литература

Волхонский В.В. «Телевизионные системы наблюдения» учеб. пособие. 2-е изд., доп. и перераб. – СПб.: Экополис и культура, 2005.

Волхонский В.В «Устройства охранной сигнализации» 3-е изд., доп. и перераб.: В 2 ч. – СПб.: Экополис и культура, 2000.

Гедзберг Ю.М. «Охранное телевидение» – М.: Горячая линия - Телеком, 2005.

Никулин О.Ю., Петрушин А.Н. «Системы телевизионного наблюдения» Учебно-справочное пособие. Под ред. Митасва В.А. – М.: Обсерв-РБ, 1997.

Под ред. М.Л.Мелик-Адамова и Н.В.Андрианова «Технические средства охраны» М.: ВИПТН МВД СССР, 1978 г.

Шепитько Г.Е., Медведев И.И. «Проблемы безопасности объектов» Учебное пособие. – М.: Академия экономической безопасности МВД России, 2006 г.

«Рекомендации по выбору и применению телевизионных систем видеоконтроля» – М.: ВНИИПО МВД России, НИЦ «Охрана», 1996

Геннадий Шанаев, Андрей Леус «Системы защиты периметра» М.:Секьюрити Фокус, 2011.-280 с.: цв.ил.

Под ред. М.Л.Мелик-Адамова и П.В.Андрианова «Технические средства охраны» – М.: ВИПТШ МВД СССР, 1978.

Видеоаналитика. Мифы и реальность. Москва "Секьюрити Фокус" 2012

Шепитько Г.Е., Медведев И.И. «Проблемы безопасности объектов» Учебное пособие. – М.: Академия экономической безопасности МВД России, 2006.

**Рекомендованные Интернет-ресурсы:**

<http://www.consultant.ru/> Справочная правовая система «Консультант Плюс»

<http://www.garant.ru/> Справочная правовая система «Гарант»

<http://www.s-director.ru/> Журнал «Директор по безопасности» специализированное ежемесячное издание, ориентированное на освещение полного комплекса проблем корпоративной безопасности: экономической, физической, технической, информационной, кадровой, юридической и т.п., а также их взаимного влияния

<http://bezopasnost-chel.ru/> Всероссийский специализированный журнал «Безопасность» отраслевое издание на рынке систем безопасности в России и Ближнем Зарубежье

<http://www.algoritm.org/> Журнал «Алгоритм безопасности» – информационно-аналитическое издание, освещающее вопросы технического обеспечения безопасности объектов

<http://www.tzmagazine.ru/> Журнал «Технология защиты» - отраслевое издание рынка технических систем безопасности. Всё о комплексных системах безопасности СКУД ОПССС TV системах пожаротушения и о других сегментах рынка ТСБ

<http://ru-bezh.ru/> РУБЕЖ информационно-аналитический журнал по теме безопасности

<http://www.mirbez.ru/> Специализированный журнал по безопасности «Мир и безопасность»

<http://www.plusworld.ru/> Информационно-аналитический журнал ПЛАС

<http://www.id-mb.ru/> Аналитический медиапортал «Мир безопасности»

<http://tek.securitymedia.ru/> Отраслевой специализированный журнал «Безопасность объектов ТЭК»

#### **4. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ**

По окончании обучения по Программе проводится итоговая аттестация в форме зачёта без оценки.

##### **Примерные вопросы для подготовки к зачёту**

1. Место и роль видеонаблюдения в системе обеспечения безопасности предприятия.
2. Основы правового использования видеонаблюдения и видеоизображений людей в деятельности подразделения безопасности предприятий ТЭК.
3. Реализация функций видеоаналитики в современных системах видеонаблюдения.
4. Особенности формирования, передачи и хранения видеoinформации в IP-сетях.
5. Открытое программное обеспечение по реализации функций видеоаналитики.
6. Современное программное обеспечение по аналитической работе с архивами видеoinформации.
7. Технические средства построения систем видеонаблюдения и регламентация их применения на объектах ТЭК.
8. Интеграция систем видеонаблюдения с другими подсистемами безопасности предприятия.
9. Методики подготовки и анализа видеoinформации при расследовании нарушений корпоративной политики безопасности.
10. Современное программное обеспечение по обработке и анализу видеoinформации.
11. Совместный анализ данных видеонаблюдения и записей электронных журналов в среде аналитических программ.



**УЧЕБНАЯ ПРОГРАММА**  
**«Повышение эффективности системы безопасности предприятия на  
основе применения видеоаналитики»**

© Негосударственное образовательное учреждение  
дополнительного профессионального образования  
«Центр предпринимательских рисков»