



Негосударственное образовательное учреждение  
дополнительного профессионального образования  
«ЦЕНТР ПРЕДПРИНИМАТЕЛЬСКИХ РИСКОВ»



УТВЕРЖДАЮ  
Директор НОУ ДПО "ЦПР"  
В.Г.Казанцев  
"23" июля 2015 года

Программа повышения квалификации

«Управление информационной безопасностью  
с использованием продукта HP ArcSight»

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 «**Управление информационной безопасностью с использованием продукта HP ArcSight**» (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).

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

## **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:

- ведущих (главных) специалистов и специалистов служб безопасности (информационной безопасности),
- руководителей и сотрудников отделов автоматизации, вычислительных центров, информационно-технических отделов,
- руководителей и сотрудников специализированных подразделений по защите конфиденциальной информации,
- администраторов безопасности компьютерных сетей, сотрудников подразделений безопасности и IT-подразделений,
- Ответственных за информационную безопасность, а также лиц включенных в резерв кадров на замещение этих должностей

Целью реализации Программы является повышение компетентности специалистов в области использования системы сбора и обработки событий информационной безопасности на базе решений HP ArcSight ESM, возможностей по мониторингу событий, выявлению и расследованию инцидентов информационной безопасности.

Программа повышения квалификации предусматривает формирование у слушателей теоретических и практических знаний в области использования системы сбора и обработки событий информационной безопасности на базе решений HP ArcSight ESM.

Особое внимание уделено мониторингу событий, выявлению и расследованию инцидентов информационной безопасности.

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 деятельности;
- 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 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-14).

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  
«Управление информационной безопасностью с использованием  
продукта HP ArcSight»

**Цель:** повышение компетентности специалистов в области использования системы сбора и обработки событий информационной безопасности на базе решений HP ArcSight ESM, возможностей по мониторингу событий, выявлению и расследованию инцидентов информационной безопасности.

**Категория слушателей:** ведущие (главные) специалисты и специалисты служб безопасности (информационной безопасности), руководители и сотрудники отделов автоматизации, вычислительных центров, информационно-технических отделов, руководители и сотрудники специализированных подразделений по защите конфиденциальной информации, администраторы безопасности компьютерных сетей, сотрудники подразделений безопасности и IT-подразделений, ответственные за информационную безопасность.

**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                | Введение.<br>Классификация продукта, назначение SIEM-систем | 2                                   | 2              |   |  |
| 2                | Обзор версий и компонентов решения                          | 4                                   | 4              | 2 |  |
| 3                | Варианты архитектуры  | 4                                   | 2              | 2 |  |
| 4                | Задачи администрирования решения                            | 4                                   | 2              | 2 |  |
| 5                | Жизненный цикл события ИБ в ArcSight                        | 4                                   | 2              | 2 |  |
| 6                | Обзор консоли ArcSight SmartConsole:<br>Ресурсы ArcSight    | 6                                   | 4              | 2 |  |



|    |  |           |           |           |                             |
|----|--|-----------|-----------|-----------|-----------------------------|
| 7  | <b>Workflow —<br/>последовательность действий<br/>при расследовании<br/>инцидентов.</b>    | 2         | 2         |           |                             |
| 8  | <b>Встроенные ресурсы ArcSight<br/>Express.<br/>Настройка правил<br/>корреляции.</b>       | 4         | 2         | 2         |                             |
| 9  | <b>Принципы разработки<br/>нестандартных коннекторов<br/>Flex-connectors.</b>              | 4         | 2         | 2         |                             |
| 10 | <b>Порядок установки<br/>компонентов ArcSight.<br/>Структура базы данных<br/>ArcSight.</b> | 4         | 2         | 2         |                             |
|    | <b>Итоговая аттестация</b>   | 2         |           | 2         | <b>Зачет<br/>без оценки</b> |
|    | <b>Итого</b>   | <b>40</b> | <b>24</b> | <b>16</b> |                             |

## 2.2. Содержание Программы

### Учебная программа повышения квалификации «Управление информационной безопасностью с использованием продукта HP ArcSight »

#### **Тема 1. Введение. Классификация продукта, назначение SIEM-систем.**

Обоснование актуальности использования SIEM-систем.

Проблемы и задачи, решаемые SIEM-системами (Схема сбора, обработки и визуализации системы ArcSight).

#### **Тема 2. Обзор версий и компонентов решения.**

ESM (на Oracle и на Corr-Engine) (входящие компоненты — WEB, СУБД, Manager, партиции БД ArcSight. ArcSight Express — 20 мин

SmartConnector (виды, поддерживаемые платформы, удаленный сбор).

Connector Appliance . ArcSight Logger. Средства визуализации — SmartConsole. Средства визуализации — Web консоли. Виды поставки системы (ПО, программно-аппаратные комплексы). Документация по продуктам.

#### **Тема 3. Варианты архитектуры.**

SSL коммуникация. Практическое занятие: Установка агента (настройка сбора с Windows/RHEL). Настройка SSL коммуникации.

#### **Тема 4. Задачи администрирования решения.**

Ролевая модель. Сетевая модель. Ценности (Assets). Зоны (Zones). Сети (Networks). Потребители (Customers). Модель ценностей. Уязвимости (Vulnerabilities). Местонахождения (Locations). Категории ценностей (Asset Categories).

#### **Тема 5. Жизненный цикл события ИБ в ArcSight.**

Сбор. Нормализация. Фильтрация. Агрегация. Приоритезация. Категоризация. Корреляция. Визуализация. Долговременное хранение. Практическое задание: Создание ценностей (Assets). Создание учетных записей пользователей и разграничение прав доступа.

#### **Тема 6. Обзор консоли ArcSight SmartConsole: Ресурсы ArcSight.**

Активные каналы. Активные листы. Листы сессий. Панели инструментов, мониторы данных. Отчеты. Уведомления. Правила корреляции. Переменные.

**Тема 7. Workflow — последовательность действий при расследовании инцидентов**  
Создание активных каналов. Создание активных листов. Создание листов сессий. Создание Панели инструментов, мониторов данных. Создание отчетов.

#### **Тема 8. Встроенные ресурсы ArcSight Express . Настройка правил корреляции.**

Создание уведомлений, настройка автоматического оповещения пользователей об инцидентах ИБ. Настройка условий для правил корреляции.

#### **Тема 9. Принципы разработки нестандартных коннекторов Flex-connectors.**

Установка и настройка нестандартного коннектора Flex-connector.

**Тема 10. Порядок установки компонентов ArcSight . Структура базы данных ArcSight.**

Схема данных. Ротация данных. Архивирование событий ИБ, работа с архивами, онлайн и оффлайн архивы. Резервное копирование основных компонентов решения. Диагностика и решение возникающих проблем (конфигурационные файлы агентов, менеджера, инструментарий СУБД, причины и диагностика неполадок). Практика: Экспорт и импорт наборов ресурсов ArcSight. Экспорт и импорт архивов событий ИБ

### **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 информационной 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-диск 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 Составы 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

Ярочкин В.И Информационная безопасность: Учебник для студентов вузов. 2-е изд. – М.: Академический Проект; Гаудеамус, 2004.

В.А. Северин "Комплексная защита информации на предприятии" 2008г.

Шаньгин В.Ф. "Защита информации в компьютерных системах и сетях" 2012г.

Конеев И.Р., Беляев А.В Информационная безопасность предприятия. – СПб.: БХВ-Петербург, 2003.

Корнеев И.К., Степанов Е.А. Защита информации в офисе: учеб. – М.: Проспект, 2008.

Липатников В.А., Стародубцев Ю.И. Защита информации. – СПб.: ВУС, 2001.

Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов. – М.: Горячая линия - Телеком, 2004

А.Е. Давыдов Р.В. Максимов О.К. Савицкий Технические средства и методы защиты информации от утечки по техническим каналам на объектах информатизации. С-Пб 2012.

М.А.Борисов, О.А.Романов Основы организованно-правовой защиты информации. Москва URSS книжный дом "ЛИБРОКОМ" 2012

**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/>RUBЕЖ 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 Классификация продукта.
- 2 Назначение SIEM-систем.
- 3 Обоснование актуальности использования SIEM-систем.
- 4 Проблемы и задачи, решаемые SIEM-системами.
- 5 Варианты архитектуры.
- 6 Задачи администрирования.
- 7 Ролевая модель.
- 8 Сетевая модель.
- 9 Модель ценностей.
- 10 Жизненный цикл события ИБ в ArcSight.
- 11 Ресурсы ArcSight.
- 12 Встроенные ресурсы ArcSight Express.
- 13 Принципы разработки нестандартных коннекторов Flex-connectors.
- 14 Структура базы данных ArcSight.
- 15 Резервное копирование основных компонентов решения.
- 16 Конфигурационные файлы агентов, менеджера, инструментарий СУБД, причины и диагностика неполадок.
- 17 Экспорт и импорт наборов ресурсов ArcSight.
- 18 Экспорт и импорт архивов событий ИБ.
- 19 Виды поставки системы (ПО, программно-аппаратные комплексы).
- 20 Workflow — последовательность действий при расследовании инцидентов.

**УЧЕБНАЯ ПРОГРАММА**  
**«Управление информационной безопасностью с использованием**  
**продукта HP ArcSight»**

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