



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
«7» августа 2015 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
«2830_ Разработка безопасности для сетей Microsoft»

Цель программы: Формирование знаний и навыков, необходимых для проектирования системы информационной безопасности инфраструктуры корпоративной сети.

Категория слушателей: Руководители и специалисты ИТ-подразделений и служб информационной безопасности, разрабатывающие политики и процедуры информационной безопасности корпоративной информационной системы.

Трудоемкость обучения: 24 академических часа.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Введение в проектирование системы информационной безопасности.	1	1		
2.	Создание плана защиты сети.	2	1	1	
3.	Определение угроз для безопасности сети.	1		1	
4.	Анализ рисков информационной безопасности.	1		1	
5.	Создание плана защиты физических ресурсов.	2		2	
6.	Создание плана защиты компьютеров.	2	1	1	
7.	Создание плана защиты учетных записей.	2		2	
8.	Создание плана защиты для аутентификации.	2		2	
9.	Создание плана защиты данных.	2	1	1	
10.	Создание плана защиты для передачи данных.	1		1	
11.	Создание плана защиты сетевых периметров.	2		2	
12.	Разработка ответных действий на инциденты безопасности.	2		2	
	Итоговая аттестация	4		4	Выполнение лабораторной работы
	Итого	24	6	18	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
«7» августа 2015 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
«СЕН1_ Сертифицированный этичный хакер»

Цель программы: Формирование знаний и навыков, необходимых для успешного предупреждения компьютерных инцидентов и устранения проблем безопасности.

Категория слушателей:

- системные администраторы безопасности, инженеры и аудиторы;
- квалифицированные специалисты в области информационных технологий.

Трудоемкость обучения: 40 академических часов.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Сбор информации.	2	1	1	
2.	Проведение сканирования.	2	1	1	
3.	Взлом паролей учетных записей.	2		2	
4.	Работа троянов, бэкдоров, вирусов и червей.	2	1	1	
5.	Переполнение буфера в программах.	2		2	
6.	Перехват сеанса.	2	1	1	
7.	DoS атаки.	2	1	1	
8.	Взлом веб-серверов.	2		2	
9.	Проведение SQL-инъекций.	2		2	
10.	Атака беспроводных сетей	2		2	
11.	Обход систем обнаружения вторжений, фаерволы и антивирусы.	3	1	2	
12.	Тестирование системы на проникновение.	3	1	2	
13.	Процесс проведения программно-технической экспертизы.	3	1	2	
14.	Работа с жесткими дисковыми носителями и файловыми системами.	3	1	2	
15.	Восстановление удаленных файлов и удаленных разделов.	3	1	2	
16.	Экспертиза сети, исследование журналов и трафика.	3	1	2	
	Итоговая аттестация	2		2	Экзамен
	Итого	40	11	29	



УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
**«СЕН2_ СНФИ. Выявление и расследование инцидентов
информационной безопасности»**

Цель программы: Формирование знаний и навыков, необходимых для расследования инцидентов информационной безопасности.

Категория слушателей:

- IT-специалисты, участвующие в обеспечении безопасности информационных систем, программно-технической экспертизе и реагировании на инциденты.

Трудоемкость обучения: 40 академических часа.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практичес- кие и семинарс- кие занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Программно-техническая экспертиза сегодня	1	1		
2.	Процесс проведения программно-технической экспертизы.	2	1	1	
3.	Поиск и выемка компьютеров.	1		1	
4.	Цифровая улика.	1	1		
5.	Работа специалиста оперативного реагирования.	1		1	
6.	Лаборатория для проведения программно-технической экспертизы.	2	1	1	
7.	Работа с жесткими дисковыми носителями и файловыми системами.	2		2	
8.	Экспертиза Windows.	2		2	
9.	Сбор и формирование дубликатов данных.	2		2	
10.	Восстановление удаленных файлов и удаленных разделов.	2		2	
11.	Проведение экспертизы с использованием AccessData FTK.	2		2	
12.	Проведение экспертизы с использованием EnCase.	2		2	

13.	Стеганография и экспертиза графических файлов.	2	1	1	
14.	Взлом паролей.	2		2	
15.	Сбор журналов и корреляция событий.	2	1	1	
16.	Экспертиза сети, исследование журналов и трафика.	2	1	1	
17.	Расследование атак на беспроводные сети.	2	1	1	
18.	Расследование атак на веб серверы.	2	1	1	
19.	Отслеживание почтовых сообщений, расследования преступления связанных с электронной почтой.	1	1		
20.	Экспертиза мобильных устройств.	2		2	
21.	Формирование отчетов о расследовании.	2	1	1	
22.	Как стать свидетелем-экспертом.	1	1		
	Итоговая аттестация	2		2	Экзамен
	Итого	40	12	28	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
« 7 » августа 2015 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
**«СЕНЗ_ ECSA/LPT. Сертифицированный аналитик по вопросам
безопасности информационных систем»**

Цель программы: Формирование знаний и навыков, необходимых для успешного расследования компьютерных инцидентов и устранения проблем безопасности.

Категория слушателей:

- системные администраторы безопасности, инженеры и аудиторы;
- квалифицированные специалисты в области информационных технологий.

Трудоемкость обучения: 40 академических часов.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Программно-техническая экспертиза сегодня	1	1		
2.	Процесс проведения программно-технической экспертизы.	2	1	1	
3.	Поиск и выемка компьютеров.	1		1	
4.	Цифровая улика.	1	1		
5.	Работа специалиста оперативного реагирования.	1		1	
6.	Лаборатория для проведения программно-технической экспертизы.	2	1	1	
7.	Работа с жесткими дисковыми носителями и файловыми системами.	2		2	
8.	Экспертиза Windows.	2		2	
9.	Сбор и формирование дубликатов данных.	2		2	
10.	Восстановление удаленных файлов и удаленных разделов.	2		2	
11.	Проведение экспертизы с использованием AccessData FTK.	2		2	
12.	Проведение экспертизы с использованием EnCase.	2		2	

13.	Стеганография и экспертиза графических файлов.	2	1	1	
14.	Взлом паролей.	2		2	
15.	Сбор журналов и корреляция событий.	2	1	1	
16.	Экспертиза сети, исследование журналов и трафика.	2	1	1	
17.	Расследование атак на беспроводные сети.	2	1	1	
18.	Расследование атак на веб серверы.	2	1	1	
19.	Отслеживание почтовых сообщений, расследования преступления связанных с электронной почтой.	1	1		
20.	Экспертиза мобильных устройств.	2		2	
21.	Формирование отчетов о расследовании.	2	1	1	
22.	Как стать свидетелем-экспертом.	1	1		
	Итоговая аттестация	2		2	Экзамен
	Итого	40	12	28	



УТВЕРЖДАЮ
Ректор НОУ ДПО «Институт АйТи»
И.О. Морозов
« 4 » августа 2015 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
**«FIREWALL_ Внедрение межсетевых экранов Cisco ASA (версия 2.0)
(FIREWALL)»**

Цель программы: Формирование знаний, необходимых для развертывания и поддержки решений по защите периметра, основанных на функциях межсетевого экранирования Cisco ASA.

Категория слушателей:

- Сотрудники компаний-провайдеров
- Channel Partner/Reseller,

Трудоемкость обучения: 40 академических часов.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практичес- кие и семинарс- кие занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Введение в специализированные устройства безопасности Cisco ASA	2	2		
2.	Внедрение базовых функций Cisco ASA по обеспечению связи и управлению устройством	8	2	6	
3.	Внедрение функций Cisco ASA по контролю доступа	8	2	6	
4.	Введение в специализированные устройства безопасности Cisco ASA	6	2	4	
5.	Внедрение функций Cisco ASA по виртуализации и обеспечению высокой доступности	6	2	4	
6.	Интеграция Security Service модулей с Cisco ASA	6	2	4	
	Итоговая аттестация	4		4	Выполнение лабораторной работы
	Итого	40	12	28	



УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
«INS _ Безопасность в сетях Cisco»

Цель программы: Формирование базовых знаний и навыков, необходимых для конфигурации защитных функций, эксплуатации и управления устройствами Cisco.

Категория слушателей:

- Сетевые проектировщики и администраторы.
- Сетевые и системные инженеры, проектирующие и поддерживающие решения по безопасности, базирующиеся на Cisco IOS.
- Channel Partner/Reseller.

Трудоемкость обучения: 40 академических часов.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практичес- кие и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Введение в принципы сетевой безопасности	4	2	2	
2.	Защита периметра	6	2	4	
3.	Обеспечение безопасности с помощью межсетевого экрана Cisco IOS	8	2	6	
4.	Статические VPN соединения	6	2	4	
5.	Защита сети с помощью программной системы предотвращения вторжений (IPS), встроенной в Cisco IOS	8	2	6	
6.	Обзор методов обеспечения безопасности в локальных сетях (LAN), сетях хранения данных (SAN), для голосового трафика и на конечных устройствах	4	1	3	
	Итоговая аттестация	4		4	Выполнение лаборатор- ной работы
	Итого	40	11	29	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
«7» августа 20 15г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
«IPS _ Внедрение системы предотвращения вторжений Cisco»

Цель программы: Формирование знаний и навыков, необходимых для внедрения системы предотвращения вторжений Cisco.

Категория слушателей:

- инженеры сопровождения и технической поддержки,
- специалисты технических и инженерных служб,
- системные администраторы,
- кандидаты на получение сертификации CCSP

Трудоемкость обучения: 40 академических часов

Форма обучения: очная,

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практичес- кие и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Введение в тему курса	4	2	2	
2.	Обзор технологии предотвращения вторжений	6	2	4	
3.	Инсталляция Cisco IPS 4200 Series Sensor	6	2	4	
4.	Сигнатуры Cisco IPS	6	2	4	
5.	Дополнительная конфигурация Cisco IPS	6	2	4	
6.	Дополнительные устройства Cisco IPS	4	1	3	
7.	Обслуживание сенсоров Cisco IPS	4	1	3	
	Итоговая аттестация	4		4	Выполнение лаборатор- ной работы
	Итого	40	12	28	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
«7» августа 2015г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
**«SECURE_Обеспечение безопасности сетей с помощью
маршрутизаторов и коммутаторов Cisco (SECURE)»**

Цель программы: Формирование знаний и навыков, необходимых для обеспечения безопасности сетей, с использованием функций обеспечения безопасности, реализованных в операционной системе Cisco IOS.

Категория слушателей:

- Сетевые проектировщики и администраторы.
- Сетевые и системные инженеры, проектирующие и поддерживающие решения по безопасности, базирующиеся на Cisco IOS.
- Сотрудники компаний-провайдеров.
- Channel Partner/Reseller,

Трудоемкость обучения: 40 академических часов.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практичес- кие и семинарс- кие занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Внедрение средств обеспечения безопасности сетевой инфраструктуры	8	2	6	
2.	Внедрение средств защиты сетевого периметра от угроз с помощью маршрутизаторов Cisco	10	4	6	
3.	Внедрение средств обеспечения безопасных подключений между филиалами корпоративной сети	10	4	6	
4.	Внедрение средств обеспечения безопасного удалённого доступа с помощью маршрутизаторов Cisco	8	2	6	
	Итоговая аттестация	4		4	Выполнение лаборатор- ной работы
	Итого	40	10	30	



УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
**«SENSS _ Развертывание решений Cisco по обеспечению
безопасности границ сети (SENSS)»**

Цель программы: Систематизировать знания и навыки, необходимые для развертывания решений Cisco по обеспечению безопасности границ сети

Категория слушателей:

- Инженеры по сетевой безопасности;
- Продавцы и партнеры Cisco;
- Клиенты Cisco

Трудоемкость обучения: 40 академических часов.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практичес- кие и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Оценка возможностей VPN-подсистемы Cisco ASA Принципы защищенного дизайна	2	2		
2.	Развертывание защиты сетевой инфраструктуры	10	2	8	
3.	Развертывание NAT на Cisco IOS и Cisco ASA	6	2	4	
4.	Развертывание элементов управления угрозами на Cisco ASA	12	2	10	
5.	Развертывание элементов управления угрозами на базе программного обеспечения Cisco IOS	6	2	4	
	Итоговая аттестация	4		4	Выполнение лабораторной работы
	Итого	40	10	30	



УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
**«SIMOS _ Внедрение решений Cisco для безопасной мобильности
(SIMOS)»**

Цель программы: Систематизировать знания и навыки, необходимые для внедрения решений Cisco для безопасной мобильности

Категория слушателей:

- Инженеры по сетевой безопасности.
- Продавцы и партнеры Cisco.
- Клиенты Cisco.

Трудоемкость обучения: 40 академических часов.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практичес- кие и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Основы технологий VPN и криптография	2	2		
2.	Внедрение защищенных решений для соединений Site-to-Site	8	2	6	
3.	Внедрение решений Site-to-Site FlexVPN на основе Cisco IOS	8	2	6	
4.	Внедрение AnyConnect VPN для удаленного доступа	8	2	6	
5.	Внедрение Cisco AnyConnect VPN	8	2	6	
6.	Обеспечение безопасности оконечных устройств и политик динамического доступа	2		2	
	Итоговая аттестация	4		4	Выполнение лаборатор- ной работы
	Итого	40	10	30	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
«4» августа 2015 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
«SISAS _ Внедрение решений Cisco для безопасного доступа (SISAS)»

Цель программы: Формирование фундаментальных знаний и практических навыков в области внедрения и управления доступом к сети, используя решения на основе платформы Cisco ISE

Категория слушателей:

- Инженеры по сетевой безопасности.
- Продавцы и партнеры Cisco.
- Клиенты Cisco.

Трудоемкость обучения: 40 академических часов.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Предотвращение угроз посредством служб идентификации	4	1	3	
2.	Основы Cisco ISE	6	2	4	
3.	Расширенный контроль доступа	8	2	6	
4.	Веб-аутентификация и гостевой доступ	6	2	4	
5.	Расширенные методы контроля доступа для периферийных устройств	8	2	6	
6.	Устранение неполадок управления доступом к сети	4	1	3	
	Итоговая аттестация	4		4	Выполнение лаборатор- ной работы
	Итого	40	10	30	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
«7» августа 2015г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
**«SITCS _ Развертывание решений Cisco по контролю за угрозами
(SITCS)»**

Цель программы: Систематизировать знания и навыки, необходимые для внедрения и поддержки безопасности на брандмауэрах Cisco ASA, используя решения Cisco следующего поколения, интегрируемые в Cisco Prime Security Manager.

Категория слушателей:

- Инженеры по сетевой безопасности.
- Продавцы и партнеры Cisco.
- Клиенты Cisco.

Трудоемкость обучения: 40 академических часов.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практичес- кие и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Сервисы межсетевого экрана Cisco ASA следующего поколения	12	4	8	
2.	Шлюз Web безопасности Cisco	6	2	4	
3.	Веб-безопасность облачных сред Cisco	6	2	4	
4.	Шлюз безопасности почты Cisco	6	2	4	
5.	Системы предотвращения вторжений Cisco	6	2	4	
	Итоговая аттестация	4		4	Выполнение лаборатор- ной работы
	Итого	40	12	28	



УТВЕРЖДАЮ
Ректор НОУДИО «Институт АйТи»
И.О. Морозов
«7» августа 2015 г.

УЧЕБНЫЙ ПЛАН

дополнительной профессиональной программы
повышения квалификации

«SN010_ Многофакторная аутентификация на основе продуктов компании SafeNet (SafeNet Multi-Factor Authentication 8.x Certification Course (SafeNet MFA 8.x))»

Цель программы: формирование навыков использования USB-ключей семейства eToken, необходимых для внедрения и эксплуатации подсистемы аутентификации с использованием цифровых сертификатов и/или одноразовых паролей на основе продуктов компании SafeNet.

Категория слушателей:

- руководители и специалисты структурных подразделений организаций, использующих (или планирующих использовать) средства аутентификации семейства eToken в корпоративных информационных системах;
- специалисты партнерских организаций компании SafeNet, внедряющих решения по аутентификации с использованием цифровых сертификатов и/или одноразовых паролей.

Трудоемкость обучения: 24 академических часа.

Форма обучения: очная

Режим занятий: по 8 академических часов в день либо по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Введение в аутентификацию. Обзор решений.	1	1		
2.	Средства двухфакторной аутентификации семейства eToken.	1	1		
3.	SafeNet Authentication Client 8.1 SP1 (SAC)	2	1	1	
4.	Компоненты инфраструктуры открытых ключей в операционных системах Microsoft Windows.	4	1	3	
5.	Управление жизненным циклом смарт-карт и USB-ключей семейства eToken на основе SafeNet Authentication Manager 8.0 (SAM).	14	4	10	
	Итоговая аттестация	2		2	Экзамен в форме тестирования
	Итого:	24	8	16	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
« 7 » августа 2015 г.

УЧЕБНЫЙ ПЛАН

дополнительной профессиональной программы
повышения квалификации

«SN011_ Аутентификация с использованием цифровых сертификатов на основе продуктов компании SafeNet»

Цель программы: Формирование навыков использования USB-ключей семейства eToken, необходимых для внедрения и эксплуатации подсистемы аутентификации с использованием цифровых сертификатов на основе продуктов компании SafeNet.

Категория слушателей: руководители и специалисты структурных подразделений организаций, использующих (или планирующих использовать) средства аутентификации семейства eToken в корпоративных информационных системах.

Трудоемкость обучения: 16 академических часов.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов (модулей)	Всего часов	В том числе		Формы контроля
			Лек- ции	практичес- кие и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Введение в аутентификацию. Обзор решений	3	1	2	
2.	Средства двухфакторной аутентификации семейства eToken	3	1	2	
3.	Компоненты инфраструктуры открытых ключей в операционных системах Microsoft Windows	4	1	3	
4.	Управление жизненным циклом смарт-карт и USB-ключей семейства eToken на основе SafeNet Authentication Manager 8.0 (SAM)	4	1	3	
	Итоговая аттестация	2		2	Экзамен в форме тестирования
	Итого:	16	4	12	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
«7» августа 2015 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
**«SN012_ Аутентификация с использованием одноразовых паролей на
основе продуктов компании SafeNet»**

Цель программы: Формирование навыков использования продуктов компании SafeNet, необходимых для внедрения и эксплуатации подсистемы аутентификации с использованием одноразовых паролей.

Категория слушателей: руководители и специалисты структурных подразделений организаций, использующих (или планирующих использовать) в корпоративных информационных системах аутентификацию на основе одноразовых паролей.

Трудоемкость обучения: 16 академических часа.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов (модулей)	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Введение в аутентификацию. Обзор решений.	2	2		
2.	Средства двухфакторной аутентификации семейства eToken. Решения SafeNet с использованием одноразовых паролей.	4	1	3	
3.	SafeNet Authentication Manager 8.0 (SAM).	4	1	3	
4.	SafeWord 2008 (или SafeNet Authentication Manager Express)	4	1	3	
	Итоговая аттестация	2		2	Экзамен в форме тестирования
	Итого:	16	5	11	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
«7» августа 20 15 г.

УЧЕБНЫЙ ПЛАН

дополнительной профессиональной программы
повышения квалификации

«SN020_ Сертифицированный специалист по продукту eSafe SmartSuite 8.5»

Цель программы: Формирование навыков эффективного использования возможностей системы контентной фильтрации eSafe.

Категория слушателей:

- руководители и специалисты структурных подразделений организаций, использующих (или планирующих использовать) решения eSafe,
- специалисты партнерских организаций компании SafeNet, внедряющих решения eSafe.

Трудоемкость обучения: 16 академических часов.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов (модулей)	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Обзор решения eSafe SmartSuite 8.5.	3	2	1	
2.	Установка, настройка, масштабирование	5	1	4	
3.	Эксплуатация и устранение проблем	4	1	3	
4.	Итоговая аттестация	4		4	Экзамен (пробный)
	Итого:	16	5	11	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
«7» августа 2015г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
**«VPN_ Внедрение виртуальных частных сетей средствами Cisco ASA
(VPN)»**

Цель программы: Формирование знаний и навыков, необходимых для выбора, конфигурирования и поддержки большинства функций специализированного устройства безопасности Cisco ASA

Категория слушателей:

- Сотрудники компаний-провайдеров.
- Channel Partner/Reseller,

Трудоемкость обучения: 40 академических часов.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практичес- кие и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Оценка возможностей VPN-подсистемы Cisco ASA	4	2	2	
2.	Внедрение решений по организации IPsec VPN на базе Cisco ASA	8	2	6	
3.	Внедрение решения по организации VPN удаленного доступа средствами программного обеспечения Cisco AnyConnect на базе Cisco ASA	8	2	6	
4.	Внедрение решений по организации бесклиентного VPN удаленного доступа	8	2	6	
5.	Внедрение продвинутых вариантов решений по организации VPN на базе Cisco ASA	8	2	6	
	Итоговая аттестация	4		4	Выполнение лабораторной работы
	Итого	40	10	30	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
«7» августа 2015 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
**«ИБ001_ Правовые и нормативно-методические основы обеспечения
информационной безопасности»**

Цель программы: Формирование базовых знаний по основам информационной безопасности и информационного права.

Категория слушателей:

- руководители и ИТ-специалисты, менеджеры, администраторы безопасности систем,
- специалисты по физической и информационной безопасности,
- внутренние аудиторы и аудиторы информационных систем.

Трудоемкость обучения: 24 академических часа.

Форма обучения: очная, дневная, с отрывом от работы

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/ п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинарс- кие занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Основы информационной безопасности	4	2	2	
2.	Место и роль правовых и нормативно-методических документов в общей структуре системы обеспечения информационной безопасности	8	4	4	
3.	Практическое применение российских и международных нормативных документов для построения комплексных систем информационной безопасности	10	2	8	
	Итоговая аттестация	2		2	Экзамен в форме тестирования
	Итого	24	8	16	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
«7» августа 2015г.

УЧЕБНЫЙ ПЛАН

дополнительной профессиональной программы
повышения квалификации

«ИБ002_ Безопасность компьютерных систем и сетей»

Цель программы: Формирование знаний и навыков, необходимых для администрирования компьютерных систем и сетей, и разработки необходимой организационно-распорядительной документации.

Категория слушателей:

- сотрудники организаций и предприятий, отвечающие за администрирование информационных систем и сетей,
- администраторы информационной безопасности, специалисты по защите информации, аналитики по вопросам компьютерной безопасности

Трудоемкость обучения: 40 академических часов.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Законодательная и нормативно-методическая база обеспечения информационной безопасности	6	3	3	
2.	Управление рисками информационной безопасности	4	1	3	
3.	Внутрикорпоративная организационно-распорядительная документация	4	1	3	
4.	Концепция многоуровневой защиты	4	1	3	
5.	Обзор технологий и технических средств защиты информации	18	4	14	
	Итоговая аттестация	4		4	Экзамен в форме тестирования
	Итого	40	10	30	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
« 7 » августа 2015 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
**«ИБ010_ Информационная безопасность в деятельности
органов государственной власти»**

Цель программы: Формирование знаний и навыков, необходимых для обеспечения безопасности информации, циркулирующей в информационных системах федеральных органов государственной власти.

Категория слушателей:

- служащие органов государственной власти, эксплуатирующие государственные информационные системы и ресурсы, либо ответственные за их разработку и внедрение;
- руководители и сотрудники государственных учреждений и предприятий, обрабатывающие информацию ограниченного доступа, а так же ответственные за организацию режима информационной безопасности.

Трудоемкость обучения: 72 академических часа.

Форма обучения: очная,

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лекции	практические и семинарские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Правовое и нормативно-методическое обеспечение информационной безопасности органов государственной власти.	16	7	9	
2.	Угрозы безопасности информации в информационных системах органов государственной власти.	12	4	8	
3.	Основные требования и рекомендации по технической защите информации ограниченного доступа.	12	2	10	
4.	Обеспечение безопасности компьютерных систем и сетей.	10	1	9	
5.	Организация работ по защите информации ограниченного доступа.	18	7	11	
	Итоговая аттестация	4		4	Экзамен в форме тестирования
	Итого	72	21	51	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
« 7 » августа 20 15 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
**«ИБ011_ Информационная безопасность: Комплексное обеспечение
информационной безопасности автоматизированных систем»**

Цель программы: Формирование знаний и навыков, необходимых для обеспечения информационной безопасности с использованием шифровальных (криптографических) средств в информационных системах.

Категория слушателей:

- руководители и сотрудники государственных, муниципальных органов и организаций различных форм собственности, использующие и (или) планирующие использовать шифровальные (криптографические) средства для обеспечения информационной безопасности,
- руководители и сотрудники департаментов (управлений, отделов, служб и т.п.) IT и информационной безопасности,
- специалисты по защите информации.

Трудоемкость обучения: 104 академических часа.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Законодательная и нормативно-методическая база использования шифровальных (криптографических) средств.	16	4	12	
2.	Теоретические основы использования шифровальных (криптографических) средств.	16	11	5	
3.	Организационные мероприятия по использованию шифровальных (криптографических) средств.	8	4	4	
4.	Практическое применение сертифицированных шифровальных (криптографических) средств.	28	6	22	
5.	Выпускная квалификационная работа	32	0	32	
	Итоговая аттестация	4		4	Экзамен в форме тестирования
	Итого	104	25	79	



УТВЕРЖДАЮ
Ректор НОУДИО «Институт АйТи»
И.О. Морозов
«7» августа 2015 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
**«ИБ020_ Обеспечение комплексной защиты
конфиденциальной информации на предприятии»**

Цель программы: Формирование навыков для обеспечения комплексной защиты конфиденциальной информации на предприятии

Категория слушателей:

- руководители и сотрудники организаций различных форм собственности, физические лица, организующие и (или) осуществляющие обработку конфиденциальной информации, эксплуатирующие информационные системы и ресурсы либо ответственные за их разработку и внедрение;
- руководители и сотрудники государственных учреждений и предприятий, обрабатывающие информацию ограниченного доступа, а также ответственные за организацию режима информационной безопасности;
- руководители и сотрудники департаментов (отделов, служб) ИТ и информационной безопасности;
- специалисты по защите информации.

Трудоемкость обучения: 72 академических часа.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Основы обеспечения комплексной защиты конфиденциальной информации	12	4	8	
2.	Правовые и нормативно-методические основы защиты информации	14	4	10	
3.	Управление рисками информационной безопасности	6	2	4	
4.	Построение комплексных систем обеспечения информационной безопасности	30	8	22	
5.	Технологии обеспечения защиты информации	6	2	4	
	Итоговая аттестация	4		4	Экзамен в форме тестирования
	Итого	72	20	52	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
«7» августа 2015 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
«ИБ021_ Организация конфиденциального делопроизводства
государственных и частных компаниях»

Цель программы: Формирование навыков для организации конфиденциального делопроизводства в государственных и частных компаниях.

Категория слушателей:

- руководители и ИТ-специалисты, менеджеры, администраторы безопасности систем, специалисты по физической и информационной безопасности,
- руководители и специалисты кадровых и финансовых органов,
- внутренние аудиторы и аудиторы информационных систем.

Трудоемкость обучения: 24 академических часа.

Форма обучения: очная, дневная, с отрывом от работы

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Введение. Основы информационной безопасности. Термины и определения	2	1	1	
2.	Актуальность организации конфиденциального делопроизводства в государственных и частных компаниях	2	1,5	0,5	
3.	Нормативно-правовые основы конфиденциального делопроизводства	1	0	1	
4.	Классификация, определение ценности и маркирование информационных активов компании	3	1	2	
5.	Организация конфиденциального делопроизводства	6	2	4	
6.	Организация электронного конфиденциального документооборота	4	1	3	
7.	Особенности работы с персоналом в организации, имеющей сведения ограниченного доступа	2	0,5	1,5	
8.	Управление инцидентами, связанными с нарушением установленных правил конфиденциального делопроизводства	2		2	
	Итоговая аттестация	2		2	Экзамен в форме тестирования
	Итого	24	7	17	

УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
« 7 » августа 2015 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации

«ИБ022_ Организация процесса обработки и регулирование отношений при осуществлении проверок операторов персональных данных»

Цель программы: Формирование знаний и навыков, необходимых для обеспечения безопасности персональных данных, обрабатываемых в информационных системах государственных, муниципальных органов и организаций различных форм собственности, физических лиц, организующих и (или) осуществляющих обработку персональных данных.

Категория слушателей:

- руководители, юристы и сотрудники кадровых органов организаций и учреждений, в которых эксплуатируются ИСПДн,
- руководители (сотрудники) структурных подразделений, должностные лица, назначенные ответственными за обеспечение безопасности персональных данных,
- руководители и специалисты, непосредственно отвечающие за обеспечение информационной безопасности, защиту ПДн в информационных системах персональных данных (ИСПДн) и реализующие мероприятия по технической защите конфиденциальной информации.

Трудоемкость обучения: 24 академических часа.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинар- ные занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Правовое и нормативно-методическое регулирование деятельности по обеспечению безопасности персональных данных.	4	1	3	
2.	Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных (ИСПДн).	2	1	1	
3.	Организация работы с персональными данными на предприятии (в организации).	4	1	3	
4.	Методы и способы защиты информации в информационных системах персональных данных.	5	1	4	
5.	Организация контроля и надзора за соответствием обработки персональных данных требованиям законодательства РФ.	7	2	5	
	Итоговая аттестация	2		2	Экзамен в форме тестирования
	Итого	24	6	18	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
« 4 » августа 2015 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
«ИБ023_ Установление и реализация режима коммерческой тайны»

Цель программы: Формирование навыков, необходимых для установления и прекращения режима коммерческой тайны.

Категория слушателей:

- руководители и сотрудники, ответственные за обеспечение различных видов безопасности кадровых и финансовых органов, связанных с коммерческой тайной предприятия;
- руководители и специалисты структурных подразделений защиты информации, внедряющие или готовящиеся к внедрению режима коммерческой тайны.

Трудоемкость обучения: 16 академических часов

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Понятие коммерческой тайны. Актуальность и необходимость реализации режима коммерческой тайны	1	1	0	
2.	Правовые и нормативно-методические регуляторы деятельности по охране конфиденциальности информации, составляющей коммерческую тайну	1	1	0	
3.	Установление, изменение и прекращение режима коммерческой тайны в отношении информации, составляющей секрет производства	2	1	1	
4.	Порядок определения сведений, составляющих коммерческую тайну предприятия	1	0	1	
5.	Категорирование объектов информатизации по уровням защищённости и группам коммерческой ценности информации	1	0	1	
6.	Порядок организации защиты информации, составляющей коммерческую тайну, на объектах информатизации	2		2	

7.	Организационные меры и технические средства защиты информации, составляющей коммерческую тайну	4	1	3	
8.	Управление инцидентами, связанными с нарушением режима коммерческой тайны	2		2	
	Итоговая аттестация	2		2	Экзамен в форме тестирования
	Итого	16	4	12	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
« 4 » августа 2015 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
**«ИБ024_ Организация обработки персональных данных в компаниях и
организациях (предприятиях) различных форм собственности»**

Цель программы: Формирование знаний и практических навыков, необходимых для организации обработки и защиты персональных данных в соответствии с требованиями законодательства и органов государственного контроля и надзора (ФСБ, ФСТЭК и Роскомнадзор).

Категория слушателей: Руководители и специалисты, назначенные ответственными за организацию обработки персональных данных в организации (на предприятии).

Трудоемкость обучения: 24 академических часа.

Форма обучения: очная

Режим занятий: по 8 академических часов в день либо иной график по согласованию с заказчиком.

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинарс- кие занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Персональные данные в организации (на предприятии).	4	1	3	
2.	Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных.	16	4	12	
3.	Обеспечение безопасности персональных данных при их обработке без использования средств автоматизации.	2	1	1	
	Итоговая аттестация	2		2	Экзамен в форме тестирова- ния
	Итого	24	6	18	



УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
**«ИБ030_ Управление информационной безопасностью организации
в соответствии с требованиями международного стандарта
ISO/IEC 27002:2005»**

Цель программы: Формирование навыков управления информационной безопасностью организации.

Категория слушателей:

- руководители и специалисты департаментов (отделов, служб) информационной безопасности и информационных технологий (CIO, CSO, CISO), управления рисками, аудита и внутреннего контроля;
- сотрудники, ответственные за организацию режима информационной безопасности компании.

Трудоемкость обучения: 40 академических часов.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинарс- кие занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Правовые и нормативно-методические основы управления информационной безопасностью организации	8	3	5	
2.	Управление рисками информационной безопасности	6	2	4	
3.	Технологии защиты конфиденциальной информации и обеспечения непрерывности бизнеса	18	6	12	
4.	Аудит информационной безопасности	4	1	3	
	Итоговая аттестация	4		4	Экзамен в форме тестирования
	Итого	40	12	28	



УТВЕРЖДАЮ
Ректор НОУ ДПО «Институт АйТи»
И.О. Морозов
«7» августа 2015 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
«ИБ032_ Управление рисками информационной безопасности»

Цель программы: Формирование знаний и навыков, необходимых для оценки информационных рисков и управления ими.

Категория слушателей:

- руководители и специалисты департаментов (отделов, служб) информационной безопасности и информационных технологий, управления рисками, аудита и внутреннего контроля;
- сотрудники, ответственные за организацию режима информационной безопасности компании.

Трудоемкость обучения: 24 академических часа.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Актуальность реализации процессов управления рисками информационной безопасности (ИБ). Термины и определения	1	1	0	
2.	Основные положения правового регулирования процессов управления рисками информационной безопасности	1	1	0	
3.	Современные методики управления рисками информационной безопасности	1	1	0	
4.	Оценка рисков информационной безопасности	2	1	1	
5.	Основные этапы анализа рисков информационной безопасности	1		1	
6.	Идентификация информационных активов компании	2	0	2	
7.	Оценивание идентифицированных ресурсов с учётом требований законодательства и бизнеса	2		2	

8.	Идентификация актуальных угроз и уязвимостей	2		2	
9.	Оценка вероятности реализации угроз и уязвимостей	2	0	2	
10.	Идентификация реализованных и планируемых мер защиты информационных активов	1	0	1	
11.	Вычисление и оценивание рисков информационной безопасности	2	0	2	
12.	Принятие решений по обработке и управлению рисками ИБ	2	1	1	
13.	Планирование деятельности по управлению рисками ИБ	2	1	1	
14.	Роли и ответственность в управлении рисками ИБ	1	1	0	
	Итоговая аттестация	2		2	Экзамен в форме тестирования
	Итого	24	7	17	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
«7» августа 2015 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
«ИБ033_ Управление непрерывностью бизнеса»

Цель программы: Формирование навыков управления непрерывностью бизнеса.

Категория слушателей:

- руководители и специалисты, которые занимаются обеспечением непрерывности бизнеса, менеджментом инцидентов информационной безопасности, аудитом, предоставлением консалтинговых услуг;
- сотрудники организаций, имеющие отношение к обеспечению непрерывности бизнеса.

Трудоемкость обучения: 24 академических часа.

Форма обучения: очная, дневная, с отрывом от работы

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Введение. Основы управления непрерывностью бизнеса	6	2	4	
2.	Программа управления непрерывностью бизнеса	10	2	8	
3.	Система управления непрерывностью бизнеса	6	2	4	
	Итоговая аттестация	2		2	Экзамен в форме тестирования
	Итого	24	6	18	



УТВЕРЖДАЮ
Ректор НОУ ДПО «Институт АйТи»
И.О. Морозов
«7» августа 2015 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
«ИБ034_ Аудит информационной безопасности»

Цель программы: Формирование практических навыков для подготовки и проведения аудита информационной безопасности

Категория слушателей:

- сотрудники организаций, привлекаемые для проведения аудита информационной безопасности, эксплуатирующие информационные системы и ресурсы либо ответственные за их разработку и внедрение;
- руководители и сотрудники структурных подразделений ИБ и ИТ (CIO, CSO, CISO);
- сотрудники компаний, оказывающих консалтинговые и аутсорсинговые услуги в области ИБ.

Трудоемкость обучения: 24 академических часа.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практичес- кие и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Актуальность аудита информационной безопасности организации. Основные термины и определения	2	2	0	
2.	Правовые и нормативно-методические основы аудита информационной безопасности	2	2	0	
3.	Основные виды, способы, принципы и критерии аудита информационной безопасности	2		2	
4.	Управление программой аудита информационной безопасности	2		2	
5.	Подготовка к аудиту информационной безопасности, состав и роли участников	2	1	1	
6.	Проведение аудита информационной безопасности	5	1	4	
7.	Порядок, содержание и правила разработки документов, оформляемых на этапе подготовки, в ходе проведения и по результатам аудита ИБ	4	1	3	

8.	Использование инструментальных средств для проведения аудита защищённости информационных систем	2		2	
9.	Концепция компетентности аудиторов	1	1	0	
	Итоговая аттестация	2		2	Экзамен в форме тестирования
	Итого	24	8	16	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
«1» *августа* 2015 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
**«ИБ038_ Построение автоматизированной системы управления
информационной безопасностью с использованием продукта Security Vision»**

Цель программы: Формирование знаний и навыков, необходимых для управления процессами информационной безопасности организации с использованием продукта SecurityVision.

Категория слушателей:

- руководители и сотрудники департаментов (отделов, служб) IT и информационной безопасности;
- специалисты по защите информации.

Трудоемкость обучения: 16 академических часов.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практичес- кие и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Назначение системы	1	1		
2.	Архитектура решения	2	1	1	
3.	Портал SecurityVisionи его основные компоненты, автоматизируемые процессы управления информационной безопасностью	2	1	1	
4.	Управление инцидентами информационной безопасности	1		1	
5.	Управление рисками информационной безопасности	1		1	
6.	Управление инвентаризацией и контроль целостности	1		1	
7.	Управление документацией	2	1	1	
8.	Подготовка отчетов	1		1	
9.	Общие настройки системы	1		1	
10.	Работа с ядром системы	2	1	1	
	Итоговая аттестация	2		2	Экзамен в форме гестирования
	Итого	16	5	11	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
« 7 » августа 2015 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
«ИБ040_ Расследование компьютерных инцидентов»

Цель программы: Формирование знаний и навыков, необходимых для организации и проведения внутренних (внутрикорпоративных) расследований компьютерных инцидентов.

Категория слушателей:

- руководители организаций и предприятий (независимо от организационно-правовой формы и формы собственности);
- руководители подразделений и уполномоченные сотрудники организаций (предприятий), в обязанности которых входит выявление и перекрытие каналов утечки информации, расследование попыток несанкционированного доступа к информации ограниченного доступа, разработка необходимых нормативно-методических и организационно-распорядительных документов по вопросам защиты информации;
- сотрудники, отвечающие за администрирование информационных систем и сетей (системные администраторы);
- администраторы информационной безопасности;
- специалисты по защите информации;
- аналитики по вопросам компьютерной безопасности.

Трудоемкость обучения: 40 академических часов.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лекции	практические и семинарские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Правовая и нормативно-методическая база расследования компьютерных инцидентов	8	4	4	
2.	Источники компьютерных инцидентов	6	2	4	
3.	Технологии и средства, используемые для расследования компьютерных инцидентов	12	4	8	
4.	Основные мероприятия по организации и проведению расследований компьютерных инцидентов	12	2	10	
	Итоговая аттестация	2		2	Экзамен в форме тестирования
	Итого	40	12	28	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
«7» августа 2015 г.

УЧЕБНЫЙ ПЛАН

дополнительной профессиональной программы

повышения квалификации

«НСД001_ Эксплуатация средств защиты от НСД семейства Аккорд»

Цель программы: формирование навыков, необходимых для эффективного применения СЗИ НСД семейства «Аккорд»TM и ПСКЗИ «ШИПКА»TM при решении задач обеспечения защиты информации на объектах информатизации учреждения (организации, предприятия).

Категория слушателей: руководители и специалисты структурных подразделений организаций, использующих (или планирующих использовать), СЗИ НСД семейства «Аккорд»TM и ПСКЗИ «ШИПКА»TM.

Трудоемкость обучения: 24 академических часа.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Все го час ов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Методы и технологии защиты информации от несанкционированного доступа с использованием программно-аппаратных комплексов (ПАК) СЗИ НСД семейства «Аккорд» TM и ПСКЗИ «ШИПКА» TM	2	2	0	
2.	Базовые защитные механизмы комплексов СЗИ НСД семейства «Аккорд» TM	2		2	
3.	Установка и администрирование комплексов СЗИ НСД семейства «Аккорд-АМДЗ»	4		4	
4.	Установка и администрирование комплексов СЗИ НСД семейства «Аккорд NT/2000»	4		4	
5.	Построение систем защиты информации с использованием комплексов СЗИ НСД семейства «Аккорд NT/2000»	4		4	
6.	Подсистема распределенного аудита и управления «Аккорд-РАУ» (АРМ администратора безопасности информации)	4		4	
7.	Персональное средство криптографической защиты информации (ПСКЗИ) «ШИПКА» (Шифрование-Идентификация-Подпись-Коды Аутентификации) и технологии его применения	2		2	
	Итоговая аттестация	2		2	Экзамен в форме тестирования
	Итого	24	2	22	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
«7» августа 2015 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
**«НСД002_ Оценка эффективности системы защиты от
несанкционированного доступа»**

Цель программы: Формирование знаний и навыков, необходимых для создания и эксплуатации системы защиты информации от несанкционированного доступа.

Категория слушателей:

- руководители и сотрудники государственных, муниципальных органов, органов местного самоуправления, организаций (предприятий) различных правовых форм и форм собственности, организующие и (или) осуществляющие обработку информации ограниченного доступа;
- руководители и сотрудники департаментов (отделов, служб) IT и информационной безопасности;
- специалисты по защите информации.

Трудоемкость обучения: 24 академических часа.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Правовое, нормативное и методическое обеспечение безопасности информации	2	2		
2.	Угрозы несанкционированного доступа к информации	4	2	2	
3.	Методы, способы и средства защиты информации от несанкционированного доступа	8	2	6	
4.	Методы, способы и средства оценки защищённости от несанкционированного доступа к информации	8	2	6	
	Итоговая аттестация	2		2	Экзамен в форме тестирования
	Итого	24	8	16	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
«7» августа 2015 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
«НСД003_Token Management System 2.0: Возможности и эксплуатация системы»

Цель программы: Формирование навыков использования базовых возможностей системы управления жизненным циклом смарт-карт и USB-ключей eToken - Token Management System.

Категория слушателей:

- руководители и специалисты структурных подразделений организаций, использующих (или планирующих использовать) средства управления жизненным циклом смарт-карт и USB-ключей eToken в корпоративных информационных системах;
- специалисты организаций, внедряющих решения по управлению жизненным циклом смарт-карт и USB-ключей eToken.

Трудоемкость обучения: 16 академических часа.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Понятие жизненного цикла электронного ключа	2	1	1	
2.	Token Management System	3	1	2	
3.	Выпуск и эксплуатация электронного ключа	3	1	2	
4.	Поддержание системы одноразовых паролей при помощи TMS	2		2	
5.	Виртуальный токен	3	1	2	
6.	Отчётность в TMS	2	1	1	
	Итоговая аттестация	1		1	Экзамен в форме тестирования
	Итого	16	5	11	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
«7» августа 2015 г.

УЧЕБНЫЙ ПЛАН

дополнительной профессиональной программы

«НСД004_ Token Management System 2.0: Установка и настройка системы»

Цель программы: Формирование навыков развертывания и эксплуатации Token Management System.

Категория слушателей:

- руководители и специалисты структурных подразделений организаций, использующих (или планирующих использовать) средства управления жизненным циклом смарт-карт и USB-ключей eToken в корпоративных информационных системах;
- специалисты организаций, внедряющих решения по управлению жизненным циклом смарт-карт и USB-ключей eToken.

Трудоемкость обучения: 8 академических часов.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинарс- кие занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Установка TMS	2	0,5	1,5	
2.	Первоначальная настройка системы	2	0,5	1,5	
3.	Политики использования токенов	1		1	
4.	Настройка коннекторов	2		2	
	Итоговая аттестация	1		1	тестирование
	Итого	8	1	7	



УТВЕРЖДАЮ
Ректор НОУДИО «Институт АйТи»
И.О. Морозов
« 7 » августа 2016 г.

УЧЕБНЫЙ ПЛАН

дополнительной профессиональной программы

«НСД005_ Построение подсистемы аутентификации в информационных системах на основе продуктов eToken и Token Management System»

Цель программы: Формирование первичных навыков, необходимых для самостоятельного выбора технологии и инфраструктуры подсистемы аутентификации в корпоративной информационной системе, внедрения, эксплуатации и технической поддержки применения USB-ключей и смарт-карт eToken.

Категория слушателей: руководители и специалисты структурных подразделений организаций, использующих (или планирующих применять) средства двухфакторной аутентификации семейства eToken в корпоративных информационных системах.

Трудоемкость обучения: 8 академических часов.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинарс- кие занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Теоретические основы построения криптосредств и средств аутентификации, правовое регулирование их применения	3	2	1	
2.	Средства аутентификации семейства eToken	4	1	3	
	Итоговая аттестация	1		1	тестирование
	Итого	8	2	6	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
« 7 » августа 2015 г.

УЧЕБНЫЙ ПЛАН

дополнительной профессиональной программы

«НСД006_ Построение подсистемы аутентификации в информационных системах на основе продуктов eToken и SafeNet Authentication Manager»

Цель программы: Формирование первичных навыков, необходимых для самостоятельного выбора технологии и инфраструктуры подсистемы аутентификации в корпоративной информационной системе, внедрения, эксплуатации и технической поддержки применения USB-ключей и смарт-карт eToken.

Категория слушателей: руководители и специалисты структурных подразделений организаций, использующих (или планирующих применять) средства двухфакторной аутентификации семейства eToken в корпоративных информационных системах.

Трудоемкость обучения: 8 академических часов.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Теоретические основы построения криптосредств и средств аутентификации, правовое регулирование их применения	3	1	2	
2.	Средства аутентификации семейства eToken	4	1	3	
	Итоговая аттестация	1		1	тестирование
	Итого	8	2	6	



УТВЕРЖДАЮ
Ректор НОУ ДПО «Институт АйТи»
И.О. Морозов
«7» августа 2015 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
**«НСД007_ SafeNet Authentication Manager: Возможности, установка,
настройка и эксплуатация»**

Цель программы: Формирование навыков развертывания и эксплуатации SafeNet Authentication Manager.

Категория слушателей:

- руководители и специалисты структурных подразделений организаций, использующих (или планирующих использовать) средства управления жизненным циклом смарт-карт и USB-ключей eToken в корпоративных информационных системах;
- специалисты организаций, внедряющих решения по управлению жизненным циклом смарт-карт и USB-ключей eToken.

Трудоемкость обучения: 8 академических часов.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Установка SAM	2	0,5	1,5	
2.	Первоначальная настройка системы	2	0,5	1,5	
3.	Политики использования токенов	1		1	
4.	Настройка коннекторов	2		2	
	Итоговая аттестация	1		1	тестирование
	Итого	8	1	7	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
«7» августа 2015 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
«НСД008_ Применение системы защиты Secret Net 7. Базовый курс»

Цель программы: Формирование теоретических знаний и практических навыков, необходимых для инсталляции компонентов, настройки защитных подсистем, управления политиками безопасности, аудита и мониторинга состояний рабочих станций.

Категория слушателей:

- руководители и сотрудники подразделений Информационной безопасности,
- сотрудники, на кого возложены обязанности управления комплексом СЗИ от НСД Secret Net

Трудоемкость обучения: 24 академических часа.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Функциональные требования Secret Net 7	10	4	6	
2.	Механизмы защиты Secret Net	12	4	8	
	Итоговая аттестация	2		2	Экзамен в форме тестирования
	Итого	24	8	16	



УТВЕРЖДАЮ
Ректор НОУ ДПО «Институт АйТи»
И.О. Морозов
«7» августа 2015 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации

«НСД009_ Применение системы защиты Secret Net 7. Расширенный курс»

Цель программы: Формирование теоретических знаний и практических навыков, необходимых для диагностики и предупреждения проблемных ситуаций, навыков «тонкой» настройки механизмов защиты, способов отладки и обеспечения бесперебойной работы системы

Категория слушателей:

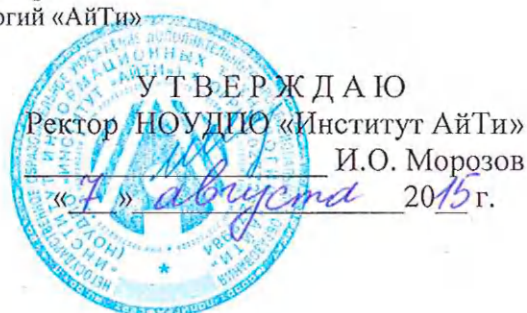
- руководители и сотрудники подразделений Информационной безопасности,
- сотрудники, на кого возложены обязанности управления комплексом СЗИ от НСД Secret Net

Трудоемкость обучения: 16 академических часов.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Дополнительные средства администрирования Secret Net 7. Вспомогательные утилиты и файлы настроек.	8	2	6	
2.	Часто встречающиеся проблемы. Диагностика и решения	6	2	4	
	Итоговая аттестация	2		2	Экзамен в форме тестирования
	Итого	16	4	12	



УТВЕРЖДАЮ
Ректор НОУДИО «Институт АйТи»
И.О. Морозов
«7» августа 2015 г.

УЧЕБНЫЙ ПЛАН

дополнительной профессиональной программы
повышения квалификации

«СЗП001_ Организация защиты периметра корпоративной сети»

Цель программы: Формирование навыков конфигурирования маршрутизаторов, межсетевых экранов, виртуальных частных сетей и других устройств, обеспечивающих безопасность периметра корпоративной сети.

Категория слушателей: руководители и сотрудники департаментов (отделов, служб) ИТ и информационной безопасности организаций.

Трудоемкость обучения: 24 академических часа.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинаре- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Стек протоколов TCP/IP	2	1	1	
2.	Понятие «многоуровневой (эшелонированной) защиты». Концепция защиты периметра корпоративной сети	2	1	1	
3.	Статическая и динамическая пакетная фильтрация	3	1	2	
4.	Списки контроля доступа маршрутизаторов	3	1	2	
5.	Межсетевые экраны	3	1	2	
6.	Трансляция адресов	3	1	2	
7.	Прокси- и сокс-серверы	3	1	2	
8.	Использование VPN-туннелей	3	1	2	
	Итоговая аттестация	2		2	Экзамен в форме тестирования
	Итого	24	8	16	

Негосударственное образовательное учреждение
дополнительного профессионального образования
«Институт информационных технологий «АйТи»

УТВЕРЖДАЮ
Ректор НОУ ДПО «Институт АйТи»
И.О. Морозов
« 7 » августа 2015 г.

УЧЕБНЫЙ ПЛАН

дополнительной профессиональной программы
повышения квалификации

«СЗП002_ Обнаружение вторжений в корпоративные сети»

Цель программы: Формирование навыков применения систем обнаружения вторжений, обеспечивающих безопасность корпоративной информационной системы.

Категория слушателей: руководители и сотрудники департаментов (отделов, служб) ИТ и информационной безопасности организаций.

Трудоемкость обучения: 24 академических часа.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Особенности протоколов TCP/IP, используемые для вредоносных целей	2	2		
2.	Применение утилиты TCPDump для анализа трафика	5	1	4	
3.	Классификация систем обнаружения вторжений	5	1	4	
4.	Система обнаружения вторжений Snort	5	1	4	
5.	Интеграция и взаимодействие СОВ с другими средствами защиты информации	5	1	4	
	Итоговая аттестация	2		2	Экзамен в форме тестирования
	Итого	24	6	18	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
« 7 » августа 2015 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
«СЗП003_ Безопасность беспроводных сетей»

Цель программы: формирование навыков, необходимых для развертывания и безопасной эксплуатации беспроводной сети организации..

Категория слушателей:

- руководители и сотрудники государственных, муниципальных органов и организаций различных форм собственности, физические лица, использующие (планирующие использовать) беспроводные сети;
- руководители и сотрудники департаментов (отделов, служб) ИТ и информационной безопасности.

Трудоемкость обучения: 24 академических часа.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинарс- кие занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Принцип работы беспроводных сетей	6	3	3	
2.	Анализ защищенности беспроводных сетей	8	2	6	
3.	Безопасность Bluetooth, организация беспроводного доступа с использованием мобильных устройств	8	2	6	
	Итоговая аттестация	2		2	Экзамен в форме тестирования
	Итого	24	7	17	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
« 7 » августа 20 15 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
«СЗП005_ Анализ защищенности сетей»

Цель программы: Формирование навыков работы со средствами мониторинга сетей, программных продуктов для анализа защищенности сетей и разработке комплекса программно-технических мер по повышению защищенности сетей.

Категория слушателей:

- руководители и сотрудники государственных, муниципальных органов и организаций различных форм собственности, физические лица, организующие и (или) осуществляющие обработку информации;
- руководители и сотрудники департаментов (отделов, служб) ИТ и информационной безопасности;
- специалисты по защите информации.

Трудоемкость обучения: 24 академических часа.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Нормативные документы, регламентирующие процедуру анализа защищенности	4	4		
2.	Анализ защищенности сетей	10	2	8	
3.	Меры по обеспечению безопасности сетей	8	2	6	
	Итоговая аттестация	2		2	Экзамен в форме тестирования
	Итого	24	8	16	



УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
**«СКЗИ001_Теория и практика использования средства
криптографической защиты информации «КриптоПро CSP»**

Цель программы: Формирование знаний и навыков, необходимых для организации и обеспечения функционирования средства криптографической защиты информации «КриптоПро CSP».

Категория слушателей: руководители и специалисты структурных подразделений организаций, использующих (или планирующих использовать) средство криптографической защиты информации «КриптоПро CSP».

Трудоемкость обучения: 16 академических часов.

Форма обучения: очная, дневная, с отрывом от работы

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Знакомство с предметом криптографической защиты информации	3	1	2	
2.	Концепция инфраструктуры открытых ключей (PKI)	3	1	2	
3.	Правовое регулирование применения СКЗИ и ЭЦП в корпоративных информационных системах	2	2		
4.	Практическая реализация СКЗИ и ЭЦП на платформе ОС Windows	3		3	
5.	СКЗИ «КриптоПро CSP»: установка, настройка, использование	4	1	3	
	Итоговая аттестация	1		1	Экзамен в форме тестирования
	Итого	16	5	11	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
«7» августа 2015 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
**«СКЗИ002_ Построение системы юридически значимой электронной
цифровой подписи в сети организации с использованием продуктов ООО
«КриптоПро»**

Цель программы: формирование практических навыков развертывания, первичной настройки и начальной эксплуатации ПАК «КриптоПро УЦ».

Категория слушателей: руководители и специалисты ИТ-подразделений и подразделений информационной безопасности организаций, использующих (или планирующих использовать) средства криптографической защиты информации (СКЗИ) и электронной подписи (ЭП), а также использующих (или планирующих использовать) ПАК «КриптоПро УЦ» в корпоративных информационных системах.

Трудоемкость обучения: 40 академических часов.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинаре- чные занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Криптографические методы защиты информации	2	2		
2.	Инфраструктура открытых ключей (ИОК/РКИ)	2	1	1	
3.	Стандарты в области РКИ	3	1	2	
4.	Протоколы и приложения РКИ	3	1	2	
5.	Правовое регулирование применения СКЗИ и ЭЦП в корпоративных информационных системах	2	2		
6.	Практическая реализация СКЗИ и ЭЦП на платформе ОС Windows	3		3	
7.	СКЗИ «КриптоПро CSP»	1,5	0,5	1	
8.	ПАК «Удостоверяющий Центр КриптоПро УЦ»	1,5	0,5	1	
9.	Установка ПАК «Удостоверяющий Центр КриптоПро УЦ»	11	3	8	
10.	Первичная настройка Центра Сертификации	1		1	

11.	Первичная настройка Центра Регистрации	1		1	
12.	Формирование и управление ключами и сертификатами пользователей с использованием АРМ администратора ЦР и АРМ пользователя ЦР	4	1	3	
13.	Использование выпущенных сертификатов пользователей в прикладных программах	1		1	
14.	Использование АРМ разбора конфликтных ситуаций	2		2	
	Итоговая аттестация	2		2	Экзамен в форме тестирования
	Итого	40	12	28	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
«7» августа 2015г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
**«СКЗИ003_ Правовое регулирование и нормативно-методическое
обеспечение деятельности удостоверяющего центра и использования
электронной подписи в информационных системах»**

Цель программы: формирование знаний, необходимых для развертывания и успешного функционирования удостоверяющего центра и/или использования электронной подписи в корпоративной информационной системе..

Категория слушателей: руководители организаций, а также руководители и специалисты подразделений информационной безопасности и ИТ-подразделений организаций, использующих (или планирующих использовать) СКЗИ и ЭП в корпоративных информационных системах, а также осуществляющих (или планирующих осуществлять) деятельность в качестве удостоверяющего центра.

Трудоемкость обучения: 16 академических часов

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком.

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Теоретические основы применения криптографических методов защиты информации	1,5	1	0,5	
2.	Концепция инфраструктуры открытых ключей (ИОК/РКИ).	1,5	1	0,5	
3.	Правовое регулирование применения СКЗИ и ЭП в корпоративных информационных системах	1,5	0,5	1	
4.	Руководящие документы ФСБ и ФСТЭК России	2		2	
5.	Удостоверяющий центр как субъект права	1,5	0,5	1	
6.	Комплекс организационно-технических мероприятий по планированию, развертыванию и эксплуатации удостоверяющего центра	2	1	1	
7.	Состав комплекта организационной, распорядительной и исполнительной документации удостоверяющего центра	1,5		1,5	

8.	Регламенты удостоверяющего центра	2	1	1	
9.	Состав комплекта организационной, распорядительной и исполнительной документации по использованию ЭП в корпоративных информационных системах	1,5		1,5	
	Итоговая аттестация	1		1	Экзамен в форме тестирования
	Итого	16	5	11	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
«7» августа 2015 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
**«СКЗИ007_ Обеспечение применения электронной подписи и
инфраструктуры открытого ключа с использованием продуктов ООО
«КРИПТО-ПРО».**

Цель программы: Формирование практических навыков развертывания, настройки и эксплуатации ПАК «КриптоПро УЦ», дополнительных Служб удостоверяющего центра и системы управления жизненным циклом функциональных ключевых носителей eToken.

Категория слушателей:

- руководители и специалисты (работники) организаций (удостоверяющих центров), использующих (или планирующих использовать) ПАК «КриптоПро УЦ», в т.ч. в корпоративных информационных системах,
- работники удостоверяющих центров, планирующих пройти аккредитацию (аккредитованных УЦ), непосредственно осуществляющие деятельность по созданию и выдаче сертификатов ключей проверки электронных подписей (для выполнения требования подпункта 4 пункта 3 статьи 16 Федерального закона «Об электронной подписи» № 63-ФЗ от 06 апреля 2011 г.).

Трудоемкость обучения: 72 академических часа.

Форма обучения: очная, дневная, с отрывом от работы

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Криптографические методы защиты информации.	2	2		
2.	Инфраструктура открытых ключей (ИОК/РКИ).	4	1	3	
3.	Стандарты в области ИОК/РКИ.	4	1	3	
4.	Протоколы и приложения ИОК/РКИ.	4	1	3	
5.	Правовое регулирование применения СКЗИ и ЭП в корпоративных информационных системах.	4	1	3	
6.	Практическая реализация СКЗИ и ЭП на платформе ОС MS Windows.	4	1	3	
7.	СКЗИ «КриптоПро CSP».	4	1	3	

8.	Программно-аппаратный комплекс «Удостоверяющий Центр КристоПро УЦ».	4	1	3	
9.	Установка ПАК «Удостоверяющий Центр КристоПро УЦ».	4	1	3	
10.	Первичная настройка Центра Сертификации.	4	1	3	
11.	Первичная настройка Центра Регистрации.	4	1	3	
12.	Формирование и управление ключами и сертификатами пользователей с использованием АРМ администратора ЦР и АРМ пользователя ЦР.	4	1	3	
13.	Использование выпущенных сертификатов пользователей в прикладных программах.	4	1	3	
14.	Использование АРМ разбора конфликтных ситуаций.	4	1	3	
15.	Выполнение регламентных процедур оператором Удостоверяющего центра.	8	2	6	
16.	Автоматизация управления жизненным циклом сертификатов, изданных с помощью «КристоПро УЦ».	4	1	3	
17.	Использование дополнительных служб в инфраструктуре открытых ключей.	4	1	3	
	Итоговая аттестация	2		2	Экзамен в форме тестирования
	Итого	72	19	53	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
«7» августа 2015 г.

УЧЕБНЫЙ ПЛАН

дополнительной профессиональной программы
повышения квалификации

«СКЗИ013_ Системы защиты конфиденциальной информации Secret Disk»

Цель программы: формирование навыков практического использования программного обеспечения семейства Secret Disk, его эффективного применения и решения возникающих при эксплуатации проблем.

Категория слушателей:

- руководители и специалисты структурных подразделений организаций, использующих (или планирующих использовать) средства обеспечения безопасности конфиденциальной информации с помощью технологий шифрования в корпоративных информационных системах,
- специалисты партнерских организаций компании Aladdin R.D., внедряющих решения по обеспечению безопасности конфиденциальной информации с помощью продуктов семейства Secret Disk.

Трудоемкость обучения: 16 академических часов.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Теоретические основы построения криптосредств и средств аутентификации, правовое регулирование их применения	3	1,5	1,5	
2.	Общие сведения о семействе программно-аппаратных комплексов Secret Disk	4	1,5	2,5	
3.	Применение программно-аппаратного комплекса Secret Disk 4	4	1	3	
4.	Применение программно-аппаратного комплекса Secret Disk Server NG	4	1	3	
	Итоговая аттестация	1		1	Экзамен в форме тестирования
	Итого	16	5	11	



УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
**«СКЗИ014_ Построение инфраструктуры аутентификации в
информационных системах на основе продуктов eToken и Token
Management System»**

Цель программы: Формирование знаний и навыков, необходимых для построения инфраструктуры аутентификации в информационных системах на основе продуктов eToken и Token Management System

Категория слушателей: руководители и специалисты структурных подразделений организаций, использующих (или планирующих использовать) средства двухфакторной аутентификации семейства eToken в корпоративных информационных системах.

Трудоемкость обучения: 8 академических часов.

Форма обучения: очная, дневная, с отрывом от работы

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Цели и задачи аутентификации. Обзор способов аутентификации.	0,5	0,5		
2.	Аутентификация с использованием методов асимметричной криптографии.	1	0,5	0,5	
3.	Аутентификация на основе одноразовых паролей.	1		1	
4.	Методы аутентификации в ЛВС и при удаленном доступе. Методы аутентификации при работе в Интернете.	1		1	
5.	Протоколы LM, NTLM, Kerberos. Протоколы PAP, CHAP, MS-CHAP v2, EAP, SSL.	1		1	
6.	Программная и аппаратная архитектуры eToken.	1		1	
7.	Работа с ПО eToken PKI Client.	1		1	
8.	Задачи управление жизненным циклом eToken в организации. Знакомство с eToken TMS.	1		1	
	Итоговая аттестация	0,5		0,5	тестирование
	Итого	16	5	11	



УТВЕРЖДАЮ
Ректор НОУДИО «Институт АйТи»
И.О. Морозов
«7» августа 2015 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
**«СКЗИ023_ Использование «КриптоПро IPsec»» для обеспечения
безопасности информации при передаче по каналам связи»**

Цель программы: формирование навыков использования ПО «КриптоПро IPsec» для защиты информации ограниченного доступа при передаче ее по каналам связи.

Категория слушателей: руководители и специалисты структурных подразделений организаций, использующих (или планирующих использовать) СКЗИ в корпоративных информационных системах..

Трудоемкость обучения: 16 академических часов.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

с	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лекции	практические и семинарские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Знакомство с предметом криптографической защиты информации	3	1	2	
2.	Концепция инфраструктуры открытых ключей (ИОК/РКИ)	3	1	2	
3.	Правовое регулирование применения СКЗИ в корпоративных информационных системах.	3	1	2	
4.	Практическая реализация СКЗИ на платформе ОС MS Windows	3	1	2	
5.	СКЗИ «КриптоПро IPsec»: установка, настройка, использование	3	1	2	
	Итоговая аттестация	1		1	Экзамен в форме тестирования
	Итого	16	5	11	



УТВЕРЖДАЮ
Ректор НОУ ДПО «Институт АйТи»
И.О. Морозов
«7» августа 2015 г.

УЧЕБНЫЙ ПЛАН

дополнительной профессиональной программы
«СКЗИ024_ Теория и практика использования программного продукта
«КриптоАРМ»

Цель программы: формирование навыков использования ПО «КриптоАРМ».

Категория слушателей:

- руководители и специалисты структурных подразделений организаций, использующих (или планирующих использовать) ПО «КриптоАРМ» в корпоративных информационных системах,
- специалисты партнерских организаций компании «Цифровые технологии».

Трудоемкость обучения: 8 академических часов.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинарс- кие занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Основные понятия и термины	1	1		
2.	Вопросы обеспечения юридически значимого электронного документооборота	1	1		
3.	Программное обеспечение «КриптоАРМ»	1,5	0,5	1	
4.	Работа с ПО «Крипто АРМ»: установка, настройка, использование	1,5	0,5	1	
5.	Комплексные готовые решения, включающие в своем составе ПО «КриптоАРМ».	2		2	
	Итоговая аттестация	1		1	тестирование
	Итого	8	3	5	



УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
**«СКЗИ041_Теория и практика использования средства
криптографической защиты информации «Верба-OW»**

Цель программы: формирование знаний и навыков, необходимых для организации и обеспечения функционирования средства криптографической защиты «Верба-OW».

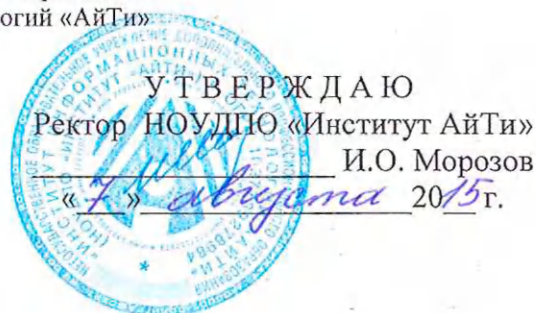
Категория слушателей: руководители и специалисты структурных подразделений организаций, использующих (или планирующих использовать) средства криптографической защиты информации и электронной подписи (ЭП) в корпоративных информационных системах.

Трудоемкость обучения: 16 академических часов.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Знакомство с предметом криптографической защиты информации	3	1	2	
2.	Концепция инфраструктуры открытых ключей (PKI)	3	1	2	
3.	Правовое регулирование применения СКЗИ и ЭП в корпоративных информационных системах	3	1	2	
4.	Практическая реализация СКЗИ и ЭП на платформе ОС MS Windows	3	1	2	
5.	СКЗИ «Верба-OW»: установка, настройка, использование	3		3	
	Итоговая аттестация	1		1	Экзамен в форме тестирования
	Итого	16	4	12	



УЧЕБНЫЙ ПЛАН

дополнительной профессиональной программы
повышения квалификации

«СКЗИ042_ Построение системы юридически значимой электронной подписи с использованием аппаратно-программного комплекса «Верба-Сертификат МВ»

Цель программы: Формирование навыков использования АПК «Верба-Сертификат МВ»

Категория слушателей: руководители и специалисты ИТ-подразделений и подразделений информационной безопасности организаций, использующих (или планирующих использовать) АПК «Верба-Сертификат МВ» в корпоративных информационных системах для создания инфраструктуры открытых ключей.

Трудоемкость обучения: 32 академических часа.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинарс- кие занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Теоретические основы применения криптографических методов защиты информации	2	2		
2.	Концепция инфраструктуры открытых ключей (ИОК/РКИ)	4	1	3	
3.	Правовое регулирование применения СКЗИ и ЭП в корпоративных информационных системах	4	1	3	
4.	СКЗИ «Верба-OW»	6	1	5	
5.	Аппаратно-программный комплекс «Верба-Сертификат МВ»	6	1	5	
	Итоговая аттестация	2		2	Экзамен в форме тестирования
	Итого	32	8	24	



УТВЕРЖДАЮ
Ректор НОУ ДПО «Институт АйТи»
И.О. Морозов
«7» августа 2015г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
«СКЗИ043_ Администрирование АПКШ «Континент» Версия 3.7. Базовый курс»

Цель программы: Формирование знаний и практических навыков, необходимых для инсталляции и управления компонентами комплекса, настройки защиты данных, передаваемых по сетям общего пользования, межсетевого экранирования и маршрутизации трафика.

Категория слушателей:

- специалисты в сфере информационной безопасности
- системные администраторы
- руководители ИТ-служб
- архитекторы систем информационной безопасности, которые отвечают за защиту каналов связи при передаче информации ограниченного доступа между сегментами сложных распределенных сетей по публичным или выделенным каналам связи

Трудоемкость обучения: 24 академических часа.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лекции	практические и семинарские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Обзор технологий и развертывание системы защиты	2	2		
2.	Управление компонентами комплекса	3	1	2	
3.	Управление политиками безопасности	3	1	2	
4.	Организация и управление VPN соединениями	4	1	3	
5.	Обеспечение отказоустойчивости комплекса	4	1	3	
6.	Мониторинг и диагностика системы защиты	2	1	1	
7.	Обновление версии программного обеспечения	4	1	3	
8.	Обзор технологий и развертывание системы защиты	2	2		
	Итоговая аттестация	2		2	Экзамен в форме тестирования
	Итого	24	8	16	



УТВЕРЖДАЮ
Ректор НОУДИО «Институт АйТи»
И.О. Морозов
«7» августа 2015 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
«СКЗИ044_ Администрирование АПКШ «Континент» Версия 3.7.
Расширенный курс»

Цель программы: Формирование знаний и практических навыков, необходимых для внедрения, настройки и обслуживания АПКШ Континент 3.7.

Категория слушателей:

- специалисты, занимающиеся внедрением, обслуживанием и администрированием систем безопасности, основанных на АПКШ «Континент 3.7»;
- сотрудники сервисных партнеров ООО «Код безопасности»;
- системные администраторы, системные инженеры, специалисты в сфере информационной безопасности и те, кто планирует пройти сертификацию по продукту АПКШ Континент 3.7.

Трудоемкость обучения: 16 академических часов.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинарс- кие занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Резервирование и отказоустойчивость каналов связи	3	1	2	
2.	Работа криптошлюза с внешними сетевыми устройствами, поддерживающими трансляцию адресов	3	1	2	
3.	Поиск и устранение неисправностей	8		8	
	Итоговая аттестация	2		2	Экзамен в форме тестирования
	Итого	16	2	14	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
«7» августа 2015 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
«СПО201_ Администрирование ОС Linux»

Цель программы: Формирование знаний и навыков, необходимых для администрирования ОС Linux.

Категория слушателей: пользователи и системные администраторы

Трудоёмкость обучения: 40 академических часов.

Форма обучения: очная,

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинарс- кие занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Введение	0,5	0,5		
2.	Основы работы с системой	1		1	
3.	Начало работы	0,5	0,5		
4.	Приложения X-Window для работы с файлами	2	1	1	
5.	Командная строка	3		3	
6.	Введение в файловую систему	4	1	3	
7.	Пользователи. Права доступа	3	1	2	
8.	Установка Linux	3		3	
9.	Установка программного обеспечения	2		2	
10.	Процесс загрузки системы и управление процессами	2		2	
11.	Окружение пользователя	1,5	0,5	1	
12.	Добавление и удаление устройств. Ядро системы	2		2	
13.	Система печати	1,5	0,5	1	
14.	Файловые системы Linux	2		2	
15.	Конфигурирование сетевых служб	8	1	7	
16.	Отличительные особенности различных дистрибутивов Linux	2	2		
	Итоговая аттестация	2		2	Экзамен в форме тестирования
	Итого	40	8	32	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
«7» августа 2015 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
«СПО202_ Безопасность ОС Linux»

Цель программы: Формирование знаний и навыков, необходимых для обеспечения безопасности в ОС Linux.

Категория слушателей:

- системные администраторы,
- сотрудники отделов информационной безопасности.

Трудоёмкость обучения: 32 академических часа.

Форма обучения: очная,

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лекции	практические и семинарские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Введение	1	1		
2.	Безопасная настройка Linux	2		2	
3.	Пользователи и аутентификация, права доступа	2	1	1	
4.	PAM, sudo	2		2	
5.	Мониторинг событий и регистрация сообщений	2	1	1	
6.	Сетевая безопасность	3	1	2	
7.	Криптография	2		2	
8.	Оптимизация системы	2		2	
9.	Резервное копирование и восстановление	2		2	
10.	Дополнительные инструменты защиты	2		2	
11.	Защита приложений	3	1	2	
12.	Настройка антивируса	2		2	
13.	Особенности безопасности различных дистрибутивов Linux	5	1	4	
	Итоговая аттестация	2		2	Экзамен в форме тестирования
	Итого	32	6	26	

УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
« 7 » *августа* 2015 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
**«ТЗКИ001_ Обеспечение безопасности персональных данных при их
обработке в информационных системах персональных данных»**

Цель программы: формирование знаний и навыков, необходимых для организации и обеспечения безопасности персональных данных, обрабатываемых в информационных системах государственных, муниципальных органов, органов местного самоуправления и организаций различных форм собственности, физических лиц, организующих и (или) осуществляющих обработку персональных данных.

Категория слушателей:

- руководители и сотрудники государственных, муниципальных органов, органов местного самоуправления, организаций различных форм собственности, физические лица, организующие и (или) осуществляющие обработку персональных данных;
- руководители и сотрудники департаментов (отделов, служб) ИТ и информационной безопасности;
- специалисты по защите информации.

Трудоемкость обучения: 72 академических часа.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практи- ческие и семинар- ские заня- тия, вы- ездные занятия и прочие виды учебных занятий и учебных работ	
1.	Организационно-правовые основы технической защиты конфиденциальной информации и обеспечения безопасности персональных данных.	10	4	6	
2.	Выявление угроз и уязвимостей безопасности персональных данных.	26	6	20	
3.	Рекомендации и основные мероприятия по организации и техническому обеспечению безопасности персональных данных.	28	8	20	
4.	Обеспечение безопасности персональных данных при их обработке без использования средств автоматизации.	6	2	4	
	Итоговая аттестация	2		2	Экзамен в форме тести- рования
	Итого	72	20	52	



УТВЕРЖДАЮ
Ректор НОУДПО «Институт АйТи»
И.О. Морозов
«7» августа 2015 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
**«ТЗКИ002_ Подготовка объектов информатизации к аттестации по
требованиям безопасности информации»**

Цель программы: сформировать у слушателей знания и навыки, которые необходимы для проведения работ по технической защите конфиденциальной информации и подготовки объектов информатизации к аттестации по требованиям безопасности информации

Категория слушателей:

- сотрудники организаций, назначенные ответственными за обеспечение режима безопасности, эксплуатацию оборудования в защищаемых помещениях и защиту конфиденциальной информации, обрабатываемой в автоматизированных системах;
- администраторы информационной безопасности (уполномоченные по защите информации);
- руководители и сотрудники департаментов (отделов, служб) ИТ и информационной безопасности;
- специалисты по защите информации.

Трудоемкость обучения: 24 академических часа.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Актуальность проблемы обеспечения технической защиты конфиденциальной информации. Основные понятия, термины и определения	1	1		
2.	Общие положения правовой и нормативно-методической базы в области защиты информации	2	1	1	
3.	Структура и основные положения «Специальных требований и рекомендаций по технической защите конфиденциальной информации» (СТР-К)	1	1		
4.	Технические каналы утечки информации, классификация и способы реализации	1		1	
5.	Угрозы несанкционированного доступа к информации	1		1	

6.	Организация работ по защите конфиденциальной информации	2	1	1	
7.	Подготовка защищаемых помещений к аттестации по требованиям безопасности информации	2	1	1	
8.	Подготовка автоматизированных систем к аттестации по требованиям безопасности информации	2	1	1	
9.	Аттестация объектов информатизации по требованиям безопасности информации. Классификация автоматизированных систем	2		2	
10.	Методики оценки защищённости конфиденциальной информации от утечки по техническим каналам	1		1	
11.	Методика аттестационных испытаний системы защиты от несанкционированного доступа	1		1	
12.	Перечень и формы документов, оформляемых заявителем в рамках аттестационных испытаний защищаемых помещений и автоматизированных систем	2		2	
13.	Перечень и формы документов, оформляемых лицензиатом по итогам каждого из этапов защиты объектов информатизации	2		2	
14.	Структура и основные задачи подразделений технической защиты информации. Должностные обязанности специалистов по защите информации	2	1	1	
	Итоговая аттестация	2		2	Экзамен в форме тестирования
	Итого	24	7	17	



УТВЕРЖДАЮ
Ректор ИОУ ДПО «Институт АйТи»
И.О. Морозов
« 7 » августа 20 15 г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
повышения квалификации
**«ТЗКИ009_Защита информации от утечки по техническим каналам.
Защита информации от несанкционированного доступа (НСД)»**

Цель программы: формирование знаний и навыков, необходимых для защиты информации в автоматизированных (информационных) системах от несанкционированного доступа (НСД).

Категория слушателей:

- сотрудники, эксплуатирующие информационные системы и ресурсы, либо ответственные за их разработку и внедрение;
- руководители и сотрудники, обрабатывающие информацию ограниченного доступа, а так же ответственные за организацию режима информационной безопасности.

Трудоемкость обучения: 72 академических часа.

Форма обучения: очная

Режим занятий: по 8 академических часов в день или по согласованию с заказчиком

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лек- ции	практиче- ские и семинар- ские занятия, выездные занятия и прочие виды учебных занятий и учебных работ	
1.	Правовое, нормативное и методическое обеспечение комплексной технической защиты информации.	10	4	6	
2.	Угрозы безопасности информации в автоматизированных системах.	30	10	20	
3.	Защита информации от несанкционированного доступа в автоматизированных системах.	30	10	20	
	Итоговая аттестация	2		2	Экзамен в форме тестирования
	Итого	72	24	48	