ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ИНКЛЮЗИВНОГОВЫСШЕГО ОБРАЗОВАНИЯ

**«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
ГУМАНИТАРНО-ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»**

КАЛМЫЦКИЙ ФИЛИАЛ

УТВЕРЖДАЮ
Директор филиала
_____Э.Л. Пашнанов
«23» 04 2020 г.

ПРОГРАММА ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ «КОРПОРАТИВНАЯ ЗАЩИТА ОТ ВНУТРЕННИХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Элиста, 2020 г.

Разработчик:

Лиджи-Гаряев Б.Б., преподаватель первой квалификационной категории, Калмыцкий филиал ФГБОУИ ВО «Московский государственный гуманитарно-экономический университет»

Рецензент:

_____Агеев С.С., заместитель начальника отдела обеспечения деятельности, противодействия коррупции кадров и защиты информации, Министерства финансов Республики Калмыкия

Рассмотрено на заседании предметно-цикловой комиссии естественнонаучных и математических дисциплин

протокол № 7 от «22» 04 2020 г.
Председатель ПЦК _____ /Катрикова Ц.Ю./

Программа обсуждена и одобрена научно-методическим советом Калмыцкого филиала ФГБОУИ ВО «Московский государственный гуманитарно-экономический университет».
Протокол № 5 от 23.04 2020 г.

Дополнительная профессиональная программа повышения квалификации «Корпоративная защита от внутренних угроз информационной безопасности» (далее – программа) определяет требования к содержанию и уровню подготовки слушателя, виды учебных занятий по реализации учебного процесса, руководство самостоятельной работой слушателей и формы контроля по данному курсу.

Программа подготовлена для индивидуальных предпринимателей и включает в себя:

1. Общая характеристика программы.

1.1.Цель реализации программы.

1.2.Задачи преподавателя программы.

1.3.Требования к уровню образования лиц, допускаемых к освоению программы.

2. Требования к результатам освоения программы.

Планируемые результаты освоения программы.

3. Содержание программы

3.1.Учебный план.

3.2.Учебно-тематический план.

4. Календарный учебный график.

5. Рабочая программа дисциплины.

6. Организационно-педагогические условия реализации программы.

6.1.Кадровое обеспечение программы.

6.2.Методические рекомендации преподавателю.

6.3.Методические указания слушателю.

7. Формы аттестации.

8. Оценочные материалы.

9. Методическое обеспечение программы.

10. Материально-техническое обеспечение программы.

1. Общая характеристика программы

1.1. Цель реализации программы

Дополнительная профессиональная программа дополнительного образования «Корпоративная защита от внутренних угроз информационной безопасности» направлена на формирование общих представлений о средствах и методах обеспечения корпоративной защиты от внутренних угроз информационной безопасности и на этой основе сформировать понимание технологий информационной безопасности и умения применять нормативно-правовую базу для классификации и расследования инцидентов, в совершенстве владеть системами и технологиями для достижения целей защиты.

Программа разработана в соответствии с:

– Федеральным законом РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.

– Федеральным законом РФ «О конкуренции и ограничении монополистической деятельности на товарных рынках» от 06.05.98 №70-ФЗ.

– Федеральным законом РФ «О рекламе» от 13.03.2006 №38-ФЗ (с учетом дополнений и изменений).

– Приказом Минобрнауки России от 01.07.2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;

– Письмом Минэкономразвития России N 5594-ЕЕ/Д28и, Минобрнауки России № АК-553/06 от 12.03.2015 «О направлении методических рекомендаций»;

– Письмом Минобрнауки России от 22.04.2015 № ВК-1032/06 «О направлении методических рекомендаций» (вместе с «Методическими рекомендациями-разъяснениями по разработке дополнительных профессиональных программ на основе профессиональных стандартов»).

1.2. Задачи программы

– формирование общих представлений о неправомерных действиях сотрудников, приводящих к потере конфиденциальных данных;

– описать общие принципы технологий, применяемых для достижения корпоративной защиты от внутренних угроз информационной безопасности;

– привить умения применять правила обеспечения защиты конфиденциальных данных организации от неправомерных утечек информации;

– освоение знаний, составляющих начала представлений об информационной картине мира и информационных процессах;

– овладение умением осуществлять сборку, установку, тестирование, использование и обслуживание специализированных программно-

аппаратных комплексов по перехвату и анализу трафика данных, циркулирующих в организации (DLP-систем);

– развитие навыков разработки политики информационной безопасности, классификации объекты защиты, понимания аспектов применения нормативно-правовой базы для классификации и расследования инцидентов.

1.3. Требования к уровню образования лиц, допускаемых к освоению программы

К освоению программы повышения квалификации допускаются:

1) лица, имеющие среднее профессиональное и (или) высшее образование;

2) лица, получающие среднее профессиональное и (или) высшее образование.

2. Требования к результатам освоения программы. Планируемые результаты освоения программы

В результате освоения программы слушатель должен обладать:

общими компетенциями, включающие в себя способность:

ОК–1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК–2. Осуществлять поиск, анализ и интерпретацию информации,

ОК–4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК–9. Использовать информационные технологии в профессиональной деятельности.

профессиональными компетенциями, соответствующие видам деятельности:

ПК- 1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

ПК-2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.

ПК-3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.

ПК-4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

В результате освоения программы обучающийся должен демонстрировать следующие результаты обучения:

знать:

– объекты компьютерных технологий, используемые в обеспечении корпоративной защиты от внутренних угроз информационной безопасности;

– понятийный аппарат информационных технологий и особенности терминологии в области корпоративной защиты от внутренних угроз информационной безопасности;

– базовые составляющие в области развития систем информационной безопасности;

– классификацию объектов защиты;

уметь:

– ставить цели, формулировать задачи, связанные с обеспечением корпоративной защиты от внутренних угроз информационной безопасности;

– анализировать тенденции развития систем обеспечения корпоративной защиты от внутренних угроз информационной безопасности;

– применять знания о корпоративной защите от внутренних угроз информационной безопасности в решении поставленных задач.

владеть:

– знаниями о современных технологиях, применяемых в области корпоративной защиты от внутренних угроз информационной безопасности;

– методами проведения анализа в области обеспечения корпоративной защиты от внутренних угроз информационной безопасности.

3. Содержание программы

3.1. Учебный план программы повышения квалификации «Корпоративная защита от внутренних угроз информационной безопасности»

Категория слушателей: специалисты, желающие освоить программу, имеющие среднее профессиональное или высшее образование, а также лица, получающие среднее профессиональное или высшее образование.

Срок обучения - 72 ч.

Форма обучения - очно-заочная

Режим занятий - 6 часов в день.

№ п/п	Наименование разделов (дисциплины, модули)	Всего, ч.	В том числе		Формы контроля
			лекции	практические занятия	
1	2	3	4	5	6
1.	Раздел 1. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз	12	4	8	Текущий контроль (устный опрос)
2.	Раздел 2. Исследование (аудит) организации с целью защиты от	12	4	8	Текущий контроль

	внутренних угроз				(устный опрос)
3.	Раздел 3. Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз	12	4	8	Текущий контроль (устный опрос)
4.	Раздел 4. Технологии анализа и защиты сетевого трафика	12	4	8	Текущий контроль (устный опрос)
5.	Раздел 5. Технологии агентского мониторинга	12	4	8	Текущий контроль (устный опрос)
6.	Раздел 6. Анализ выявленных инцидентов	6	2	4	Текущий контроль (устный опрос)
		6			демонстрационный экзамен
	ИТОГО	72	22	44	

3.2. Учебно-тематический план программы повышения квалификации «Корпоративная защита от внутренних угроз информационной безопасности»

№ п/п	Наименование разделов (дисциплины, модули)	Всего, ч.	В том числе		Формы контроля
			лекции	практические занятия	
1	2	3	4	5	6
1	**Раздел 1. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз**				
1.1.	Конфигурация сетевой инфраструктуры: настройка хостмашины, сетевого окружения, виртуальных машин, и т.п.. Установка и настройка системы корпоративной защиты от внутренних угроз. Самостоятельный поиск и устранение неисправностей при развёртывании и настройке. Установка и настройка агентского мониторинга. Проведена синхронизация с LDAP-сервером, раздел персоны заполнен корректно. Запустить систему корпоративной защиты от внутренних угроз, проверить работоспособность. Провести	12	4	8	Текущий контроль (устный опрос)

	имитацию процесса утечки конфиденциальной информации в системе.				
2.	**Раздел 2. Исследование (аудит) организации с целью защиты от внутренних угроз**				
2.1.	Угрозы информационной безопасности Самостоятельно изучить структуру организации на основании полученных материалов («модели организации»), провести обследование корпоративных информационных систем. Определить объекты защиты. Перечень субъектов/персон сформулирован верно, роли пользователей, права доступа. Определить каналы передачи данных и потенциальных утечек. Типы циркулирующих данных определены верно Выявить потоки передачи данных и возможные каналы утечки информации. Заполнить шаблон модели угроз. Подготовить отчёт о результатах аудита, включая потоки данных, потенциальные каналы утечек, уровни рисков роли пользователей, объекты защиты (с привязкой к нормативной базе и методикам оценки последствий), ролями пользователей и т.п. Определить перечень нормативных актов РФ, задействованных в рамках модели угроз. Разработать перечень, описание и шаблоны нормативно-правовых документов организации по легальному применению корпоративной защиты от внутренних угроз информационной безопасности.	12	4	8	Текущий контроль (устный опрос)
3	**Раздел 3. Разработка политик безопасности в системе корпоративной**				

	защиты информации от внутренних угроз				
3.1.	Политика безопасности Разработать новые и/или модифицировать существующие политики безопасности, перекрывающие каналы передачи данных и возможные инциденты согласно конкурсного задания. Разработать или/и модифицировать объекты защиты, категории, технологии защиты в DLP-системе и т.п. Использовать различные технологии защиты: печатей, бланков, графических объектов, баз данных и т.п. Занести политики информационной безопасности в DLPсистему Модифицировать политики безопасности в системе IWTM в соответствие с получаемыми на практике данными перехвата. Применить политики для контроля трафика, выявления и/или блокирования инцидентов безопасности, создаваемых внешним Генератором угроз. Максимизировать число выявленных инцидентов безопасности. Работа с интерфейсом управления системы корпоративной защиты информации.	12	4	8	Текущий контроль (устный опрос)
4	**Раздел 4. Технологии анализа и защиты сетевого трафика**				
4.1.	Технологии анализа и защиты сетевого трафика. Развёртывание, настройка и проверка работоспособности VPN-сети на существующей и вычислительной инфраструктуре. Развёртывание, настройка и проверка работоспособности IDS-системы на существующей и вычислительной	12	4	8	Текущий контроль (устный опрос)

	инфраструктуре. VPN. Работа с узлами и пользователями. VPN. Компрометация узлов, ключей, пользователей. Восстановление связи. Обновление ключевой информации. VPN. Межсетевое взаимодействие и туннелированные. VPN. Централизованные политики безопасности. Защита рабочих мест. IDS. Выявление большей части инцидентов безопасности за ограниченное время и/или с учётом неожиданно меняющихся условий				
5	**Раздел 5. Технологии агентского мониторинга**				
5.1.	Технологии агентского мониторинга. Продемонстрировать знание механизмов работы агентского мониторинга. Разработать и применить политики агентского мониторинга для работы с носителями и устройствами. Разработать и применить политики агентского мониторинга для работы с файлами. Работа с исключениями из перехвата	12	4	8	Текущий контроль (устный опрос)
6	**Раздел 6. Анализ выявленных инцидентов**				
6.1.	Анализ выявленных инцидентов. Подготовка отчётов о нарушениях. Применение механизмов создания фильтров для анализа перехваченного трафика и выявленных инцидентов. Проведение классификацию уровня угроз инцидентов. Оценка ущерба; Использование дополнительных модули анализа информационных потоков, если это продиктовано особенностями условий ведения бизнеса. Разработка план по дальнейшему расследованию	6	2	4	Текущий контроль (устный опрос)

	выявленных инцидентов и противодействию нарушителям с опорой на нормативную базу.				
	Итоговая аттестация.	6	**-**	**-**	**демонстрационный экзамен**
	Итого	72	22	44	

4. Календарный учебный график

Объем программы - 72 часа.

Продолжительность обучения – 2 недели, 12 рабочих дней.

Период обучения/учебные дни					
1	**2**	**3**	**4**	**5**	**6**
Р1	Р1,2	Р2,3	Р3	Р4,5	Р5
7	**8**	**9**	**10**	**11**	**12**
Р5	Р5,6	Р6	Р6	Р6	ИА

*Примечание: Р – раздел с порядковым номером в соответствии с учебным планом, ИА – итоговая аттестация.

5. Рабочая программа дисциплины

Раздел 1. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз

Конфигурация сетевой инфраструктуры: настройка хостмашины, сетевого окружения, виртуальных машин, и т.п.. Установка и настройка системы корпоративной защиты от внутренних угроз.

Практические занятия

Самостоятельный поиск и устранение неисправностей при развёртывании и настройке. Установка и настройка агентского мониторинга. Синхронизация с LDAP-сервером, раздел персоны заполнен корректно. Запустить систему корпоративной защиты от внутренних угроз, проверить работоспособность. Провести имитацию процесса утечки конфиденциальной информации в системе.

Раздел 2. Исследование (аудит) организации с целью защиты от внутренних угроз

Угрозы информационной безопасности

Практические занятия

Самостоятельно изучить структуру организации на основании полученных материалов («модели организации»), провести обследование корпоративных информационных систем. Определить объекты защиты. Перечень

субъектов/персон сформулирован верно, роли пользователей, права доступа. Определить каналы передачи данных и потенциальных утечек. Типы циркулирующих данных определены верно Выявить потоки передачи данных и возможные каналы утечки информации. Заполнить шаблон модели угроз. Подготовить отчёт о результатах аудита, включая потоки данных, потенциальные каналы утечек, уровни рисков роли пользователей, объекты защиты (с привязкой к нормативной базе и методикам оценки последствий), ролями пользователей и т.п. Определить перечень нормативных актов РФ, задействованных в рамках модели угроз. Разработать перечень, описание и шаблоны нормативно-правовых документов организации по легальному применению корпоративной защиты от внутренних угроз информационной безопасности.

Раздел 3. Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз

Политика безопасности

Практические занятия

Разработать новые и/или модифицировать существующие политики безопасности, перекрывающие каналы передачи данных и возможные инциденты согласно конкурсного задания. Разработать или/и модифицировать объекты защиты, категории, технологии защиты в DLP-системе и т.п. Использовать различные технологии защиты: печатей, бланков, графических объектов, баз данных и т.п. Занести политики информационной безопасности в DLPсистему Модифицировать политики безопасности в системе IWTM в соответствие с получаемыми на практике данными перехвата. Применить политики для контроля трафика, выявления и/или блокирования инцидентов безопасности, создаваемых внешним Генератором угроз. Максимизировать число выявленных инцидентов безопасности. Работа с интерфейсом управления системы корпоративной защиты информации.

Раздел 4. Технологии анализа и защиты сетевого трафика

Технологии анализа и защиты сетевого трафика

Практические занятия

Развёртывание, настройка и проверка работоспособности VPN-сети на существующей и вычислительной инфраструктуре. Развёртывание, настройка и проверка работоспособности IDS-системы на существующей и вычислительной инфраструктуре. VPN. Работа с узлами и пользователями. VPN. Компрометация узлов, ключей, пользователей. Восстановление связи. Обновление ключевой информации. VPN. Межсетевое взаимодействие и туннелированные. VPN. Централизованные политики безопасности. Защита рабочих мест. IDS. Выявление большей части инцидентов безопасности за ограниченное время и/или с учётом неожиданно меняющихся условий

Раздел 5. Технологии агентского мониторинга

Технологии агентского мониторинга

Практические занятия

Продемонстрировать знание механизмов работы агентского мониторинга. Разработать и применить политики агентского мониторинга для работы с носителями и устройствами. Разработать и применить политики агентского мониторинга для работы с файлами. Работа с исключениями из перехвата

Раздел 6. Анализ выявленных инцидентов

Анализ выявленных инцидентов

Практические занятия

Подготовка отчётов о нарушениях. Применение механизмов создания фильтров для анализа перехваченного трафика и выявленных инцидентов. Проведение классификацию уровня угроз инцидентов. Оценка ущерба; Использование дополнительных модули анализа информационных потоков, если это продиктовано особенностями условий ведения бизнеса. Разработка план по дальнейшему расследованию выявленных инцидентов и противодействию нарушителям с опорой на нормативную базу.

6. Организационно-педагогические условия реализации программы

6.1. Кадровое обеспечение программы

В реализации дополнительной профессиональной программы повышения квалификации «Корпоративная защита от внутренних угроз информационной безопасности» участвуют преподаватели, имеющие высшее образование, соответствующее профилю преподаваемой дисциплины и богатый опыт деятельности в области построения маркетинговых стратегий с использованием Интернет сервисов, в том числе:

Ф.И.О.	Должность	Ученая степень/ученое звание
Лиджи-Гаряев Б.Б.	Преподаватель первой категории, эксперт демонстрационного экзамена по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»	-
		-
		-

6.2. Методические рекомендации преподавателю

Программа повышения квалификации «Корпоративная защита от внутренних угроз информационной безопасности» разработана для

проведения занятий в Калмыцком филиале МГГЭУ со слушателями, из числа граждан, зарегистрированных в качестве индивидуальных предпринимателей, желающих освоить программу.

Основными видами аудиторной работы слушателей являются: лекции и практические занятия.

В ходе лекции преподаватель излагает и разъясняет основные положения темы, связанные с ней теоретические и практические проблемы, дает рекомендации к практической деятельности.

При проведении практических занятий преподаватель должен четко формулировать цель занятия и основные проблемные вопросы. После заслушивания ответов слушателей необходимо подчеркнуть положительные аспекты их работы, обратить внимание на имеющиеся неточности (ошибки), дать рекомендации по дальнейшей подготовке.

В целях контроля уровня подготовленности слушателей, для закрепления теоретических знаний и привития им навыков работы по предложенной тематике преподаватель в ходе лекции и практических занятий может проводить устные опросы, давать письменные практические задания, с помощью которых преподаватель проверяет умение применять полученные знания для решения конкретных задач.

Преподаватель должен осуществлять индивидуальный контроль работы слушателей; давать соответствующие рекомендации; в случае необходимости помочь слушателю составить индивидуальный план работы по изучению данной программы.

6.3. Методические указания слушателю

Основными видами аудиторной работы слушателей при изучении дополнительной профессиональной программы дополнительного образования «Корпоративная защита от внутренних угроз информационной безопасности» являются лекции и практические занятия.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. Слушатель не имеет права пропускать без уважительных причин аудиторные занятия, в противном случае он может быть не допущен к итоговой аттестации.

При изучении тем учебной программы применяются практические занятия, цель которых заключается в достижении более глубокого, полного усвоения учебного материала, а также развитие навыков самообразования. Кроме того, практические занятия служат формой контроля преподавателем уровня подготовленности слушателя, закрепления изученного материала, выработки навыков и умений применять полученные знания для решения имеющихся и вновь возникающих профессиональных задач.

При реализации вышеуказанных форм изучения материала курсов повышения квалификации предусматриваются следующие виды самостоятельной работы слушателей:

– работа с учебно-методическими пособиями (конспектом лекций);

– работа с рекомендованной литературой;
– работа в сети интернет;
– подготовка к итоговой аттестации.

7. Формы аттестации

Текущий контроль осуществляется преподавателем, ведущим лекционные и практические занятия, после изучения каждого модуля в виде устного опроса. Результаты текущего контроля являются допуском слушателя к итоговой аттестации или отчислению за невыполнение учебного плана.

Завершающей стадией обучения является итоговая аттестация в форме демонстрационного экзамена в виде выполнения практической работы в целях контроля уровня освоения программы. К итоговой аттестации допускается слушатель, не имеющий задолженности и в полном объеме выполнивший учебный план по программе. Итоговая аттестация может проводится как на бумажных носителях, так с использованием специальных программ. Итоговая аттестация слушателей осуществляется итоговой аттестационной комиссией, созданной Калмыцким филиалом МГГЭУ. Результаты итоговой аттестации определяются итоговой аттестационной комиссией по результатам выполненных тестовых заданий на последнем занятии.

Слушатели, успешно освоившие программу и прошедшие итоговую аттестацию, получают удостоверение о повышении квалификации.

8. Оценочные материалы

С целью проверки знаний по программе повышения квалификации «Корпоративная защита от внутренних угроз информационной безопасности» используются следующие методы: для текущего контроля - устный опрос, для итоговой аттестации - тестирование.

Оценочные материалы для текущего контроля в форме устного опроса:

1. Технологии работы с политиками информационной безопасности;
2. Создание новых политик, модификация существующих;
3. Общие принципы при работе интерфейсом системы защиты корпоративной информации;
4. Объекты защиты, персоны;
5. Ключевые технологии анализа трафика;
6. Типовые протоколы и потоки данных в корпоративной среде, такими как:корпоративная почта (протоколы SMTP, ESMTP, POP3, IMAP4), веб-почта; Интернет-ресурсы: сайты, блоги, форумы и т.д. (протоколы HTTP, HTTPS); социальные сети; интернет-мессенджеры: OSCAR (ICQ), Telegram, Jabber, XMPP, Mail.ru Агент, Google Talk, Skype, QIP; принтеры: печать файлов на локальных и сетевых принтерах; любые съемные носители и

устройства;

7. Осознание важности полноты построения политик безопасности для выявления всех возможных инцидентов и выявления фактов утечек;

8. Типы угроз информационной безопасности, типы инцидентов,

9. Технологий анализа трафика при работе политиками информационной безопасности в системе корпоративной защиты информации;

10. Основные разделы и особенности работы интерфейса управления системы корпоративной защиты информации;

11. Алгоритм действий при разработке и использовании политик безопасности, основываясь на различных технологиях анализа данных;

12. Типовые сигнатуры, используемые для детектирования файлов, циркулирующих в системах хранения и передачи корпоративной информации;

13. Роль фильтров при анализе перехваченного трафика; Технические ограничения механизма фильтрации, его преимущества и недостатки;

14. Разделы системы корпоративной безопасности, которые используются офицером безопасности в повседневной работе;

15. Особенности обработки HTTP-запросов и писем, отправляемых с помощью веб-сервисов;

16. Технологии анализа корпоративного трафика, используемые в системе корпоративной защите информации.

Текущий контроль в форме устного опроса оценивается по двухбалльной системе: «зачет», «незачет».

Критерии оценивания устного опроса:

Оценка «зачет» ставится, если:

- в ответах на вопросы при раскрытии содержания вопросов раскрываются и анализируются основные противоречия и проблемы;
- при раскрытии особенностей развития тех или иных профессиональных идей, а также описания профессиональной деятельности используются материалы современных пособий и первоисточников, допускаются фактические ошибки;
- представление профессиональной деятельности в полном объеме или частично рассматривается в контексте собственного профессионального опыта, практики его организации;
- при ответе используется терминология и дается ее определение, соответствующая конкретному периоду развития теории и практики профессиональной деятельности;
- ответы на вопросы имеют логически выстроенный характер, используются такие мыслительные операции, как сравнение, анализ и обобщение;
- имеется личная точка зрения слушателя, основанная на фактическом и проблемном материале, приобретенной на лекционных и практических занятиях и в результате самостоятельной работы.

Оценка «незачет» ставится, если:

- при ответе обнаруживается отсутствие владением материалом в объеме изучаемой образовательной программы;
- при раскрытии особенностей развития тех или иных профессиональных идей не используются материалы современных источников;
- представление профессиональной деятельности не рассматривается в контексте собственного профессионального опыта, практики его организации;
- при ответе на вопросы не дается трактовка основных понятий;
- ответы на вопросы не имеют логически выстроенного характера, не используются такие мыслительные операции, как сравнение, анализ и обобщение.

Оценочные материалы для итоговой аттестации:

Модуль 1: Анализа информационного пространства

Цель участника – разработать политики информационной безопасности, используя инструментарий автоматизированной системы IWTM 6 и успешно их применить для выявления и/или блокирования инцидентов безопасности. Для создания инцидентов и других событий в IWTM используется специальное программное обеспечение – специальный Генератор трафика и инцидентов. Участнику необходимо:

1. Разработать новые и/или модифицировать существующие политики безопасности, перекрывающие каналы передачи данных и возможные инциденты согласно конкурсного задания;
2. Занести политики информационной безопасности в DLP-систему;
3. Разработать или/и модифицировать объекты защиты, категории, технологии защиты в DLP-системе и т.п.;
4. Применить политики для контроля трафика, выявления и/или блокирования инцидентов безопасности, создаваемых внешним Генератором трафика и инцидентов. Максимизировать число выявленных инцидентов безопасности;
5. Продемонстрировать владение технологиями и умение работать с интерфейсом управления системы корпоративной защиты информации IWTM. Участнику необходимо применить политики информационной безопасности в системе IWTM, автоматически выполнить поиск инцидентов информационной безопасности, внесенных членами жюри (с использованием стенда и Генератора трафика и инцидентов). Политики можно модифицировать, с целью выявления максимального числа инцидентов и утечек. Необходимо использовать весь набор технологий поиска и выявления уязвимостей, доступный в системе корпоративной защиты. Итоговый вариант политик должен быть зафиксированы в отчете. В число инцидентов могут входить, например:

– передача персональных данных сотрудников и контрагентов по электронной почте;

– передача базы клиентов организации в архиве с использованием файловых протоколов;

– нецензурная лексика сотрудников в переписке с контрагентами;

– передача информации, составляющей коммерческую тайну и др. Задание выполняется с помощью программного обеспечения DLP (Data Leaks Prevention) IWTM 6.

Критерии оценивания итоговой аттестации:

Общее максимально возможное количество баллов задания по всемкритериям оценки составляет 36, 95.

№ п/п	Критерий	Модель в котором используются критерии	Проверяемые разделы WSSS	Баллы		
				Судейская (если это применимо)	Объективная	Общая
1	A Анализаинформационного пространства	1	1, 2, 3	2,00	23,40	25,40
2	B Разработкастратегиипродвижения	2	1, 2, 3, 5	1,00	1055	11,55
Итого =				**3,00**	**33,95**	**36,95**

9. Методическое обеспечение программы

9.1. Нормативные правовые акты

1. Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.

9.2. Дополнительная литература

1. Безбогов А.А., Яковлев А.В., Мартемьянов Ю.Ф. Безопасность операционных систем. М.: Гелиос АРВ, 2008.

2. Борисов М.А. Особенности защиты персональных данных в трудовых отношениях. М.: Либроком, 2012. – 224 с.

3. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации: Учебник для вузов. 2-е изд. - СПб.: Питер, 2006 - 703 с.

4. ГубенковА.А.Информационная безопасность вычислительных сетей: учеб. пособие / А. А. Губенков. - Саратов: СГТУ, 2009. - 88 с.

5. Дейтел Х. М., Дейтел П. Дж., Чофнес Д. Р. Операционные системы. Часть 1. Основы и принципы – М.: Бином, 2011. – 1024 с.

6. Дейтел Х. М., Дейтел П. Дж., Чофнес Д. Р. Операционные системы. Часть 2. Распределенные системы, сети, безопасность – М.: Бином, 2011. – 704 с.

7. Иванов В.И., Гордиенко В.Н., Попов Г.Н. Цифровые и аналоговые системы передачи: Учебник.-М.: Горячая линия-Телеком., 2008

8. Кофлер М., Linux. Полное руководство – Питер, 2011. – 800 с.

9. Кулаков В.Г., Гагарин М.В., и др. Информационная безопасность телекоммуникационных систем. Учебное пособие.-М.: Радио и связь, 2008

10. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: Учебное пособие.- 2-е изд., испр.- М.: Интернет-Университет ИТ; БИНОМ. Лаборатория знаний, 2007.- 531 с.

11. Мак-Клар С., Скембрей Дж., Куртц Д. Секреты хакеров. Безопасность сетей – готовые решения, 4-е изд. – М.: Вильямс, 2004. – 656 с.

12. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: Учеб. Пособие для вузов.- 3-е изд., стер. М.: Горячая линия, 2005.- 147 с.

13. Мельников Д. Информационная безопасность открытых систем.- М.: Форум, 2013.

14. Партыка Т. Л., Попов И. И. Операционные системы, среды и оболочки: учеб. пос. для студентов СПО – М.: Форум, 2013. – 544 с.

15. Платонов, В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей: Учеб. пособие для студ. высш. учеб. заведений / В. В. Платонов. – М.: Академия, 2006. – 240 с.

16. Руссинович М., Соломон Д., Внутреннее устройство MicrosoftWindows. Основные подсистемы операционной системы – Питер, 2014. – 672 с.

17. Северин В. Комплексная защита информации на предприятии. М.: Городец, 2008. – 368 с.

18. Синицын С.В. , Батаев А.В. , Налютин Н.Ю. Операционные системы – М.: Издательский центр «Академия», 2013.

19. Скрипник Д. А. Общие вопросы технической защиты информации: учебное пособие / Скрипник Д. А. –М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.

9.2.Интернет - ресурсы:

1. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru

2. Информационный портал по безопасности www.SecurityLab.ru.

3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/

4. Российский биометрический портал www.biometrics.ru

5. Сайт журнала Информационная безопасность http://www.itsec.ru –

6. Сайт Научной электронной библиотеки www.elibrary.ru

7. Справочно-правовая система «Гарант» » www.garant.ru

8. Справочно-правовая система «Консультант Плюс» www.consultant.ru

9. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

10. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru

11. Федеральный портал «Российское образование www.edu.ru

10. Материально-технические условия реализации программы

Учебно-методическое обеспечение:

– набор электронных презентаций для использования в аудиторных занятиях;

– тестовые материалы (для проведения электронного тестирования);

– дидактические материалы в электронном виде;

– набор оценочных средств для контроля усвоения материала по темам программы.

Материально-техническое обеспечение

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
Аудитория	Лекции	Компьютер, мультимедийный проектор, экран, интерактивная доска. Набор электронных презентаций для использования в аудиторных занятиях. МФУ. Автоматизированное рабочее место преподавателя. Автоматизированные рабочие места обучающихся.
Мастерская по компетенции «Корпоративная защита от внутренних угроз	Практические занятия	Автоматизированное рабочее место преподавателя: не менее Core i5, 8GB ОЗУ, 1TB HD, Монитор 22", ИБП на 650Вт Автоматизированные рабочие места

информационной безопасности»		обучающихся: не менее Core i5, 8GB ОЗУ, 1TB HD, Монитор 22", ИБП на 650Вт.
Мастерская по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»	Итоговая аттестация	Автоматизированное рабочее место: не менее Core i5, 8GB ОЗУ, 1TB HD, Монитор 22", ИБП на 650Вт, мультимедийный проектор, экран, интерактивная доска. Автоматизированное рабочее место преподавателя: не менее Core i5, 8GB ОЗУ, 1TB HD, Монитор 22", ИБП на 650Вт Автоматизированные рабочие места обучающихся: не менее Core i5, 8GB ОЗУ, 1TB HD, Монитор 22", ИБП на