

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

Утверждаю
Зам. директора по УР
 Н.А. Андреева
« 31 » 03 2025 г.

Рабочая программа дисциплины

Б1.В.07 Аналитика DLP-систем

Кафедра: **Информационная безопасность**
Направление подготовки: **10.03.01 Информационная безопасность**
Профиль: **Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)**
Формы обучения: **очная**

Распределение часов дисциплины по семестрам (для очной формы обучения (ОФО))

Вид учебной работы	ОФО	
	ЗЕ	часов/ семестр
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	3	108/8
Контактная работа, в том числе (по семестрам, курсам):		52/8
Лекции		18/8
Лабораторных работ		34/8
Практических занятий		
Семинаров		
Самостоятельная работа		56/8
Контроль		
Число контрольных работ (по курсам)		
Число КР (по семестрам, курсам)		
Число КП (по семестрам, курсам)		
Число зачетов с разбивкой по семестрам (курсам)		1/8
Число экзаменов с разбивкой по семестрам (курсам)		

Программу составил:

И.о. зав. кафедрой ИБ, д.пол.н., к.т.н. доцент Жуковский А.Г.

Рабочая программа дисциплины

«Аналитика DLP-систем»

Разработана в соответствии с ФГОС ВО:

направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. N 1427

Составлена на основании учебного плана

направления 10.03.01 Информационная безопасность, профиля «Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)», одобренного Учёным советом СКФ МТУСИ, протокол № 8 от 31.03.2025г., и утвержденного директором СКФ МТУСИ 31.03.2025 г.

Рассмотрена и одобрена на заседании кафедры

Информационная безопасность

Протокол от «31» 03 2025 г. № 8

И.о. зав. кафедрой  А.Г.Жуковский

1. Цели изучения дисциплины

Целью преподавания дисциплины «Аналитика DLP-систем» является формирование у обучающихся знаний в области основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования программных и аппаратных средств в сетях и информационных системах.

2. Планируемые результаты обучения

Изучение дисциплины направлено на формирование у обучающегося способности решать профессиональные задачи в соответствии с *эксплуатационным* видом деятельности:

Результатом освоения дисциплины являются сформированные у обучающегося следующие компетенции:

Компетенции, формируемые у обучающегося в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)	
ПК-3: Администрирование средств защиты информации прикладного и системного программного обеспечения	
Знать:	
- Архитектуру DLP-систем; - Принципы построения DLP-систем; - Основные средства и методы анализа работы программного комплекса DLP; - Источники угроз информационной безопасности, вызывающие утечку информации; - Характерные признаки наличия утечки информации; - Средства и методы обнаружения ранее источников утечки информации.	
Уметь:	
- Анализировать источники утечки информации; - Формулировать правила безопасной эксплуатации программного обеспечения; - Использовать программное обеспечение с целью определения возможного вредоносного воздействия; - Инсталлировать и эксплуатировать DLP-системы; - Осуществлять мероприятия по противодействию утечке информации с помощью DLP.	
Владеть:	
- Определением порядка установки программного обеспечения DLP; - Определением выбора с DLP для конкретной организации; - Формированием требований к DLP-системам; - Формированием требований к встроенным средствам определения источников утечки информации.	

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Б1.О.32 Основы управления информационной безопасностью,
2	Б1.О.28 Организационное и правовое обеспечение информационной безопасности,
3	Б1.О.24 Искусственный интеллект и машинное обучение в кибербезопасности,
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б1.О.36.06 Администрирование средств защиты информации в компьютерных системах и сетях,
2	Б1.В.02 Комплексное обеспечение защиты информации объекта информатизации.

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 108 часов, 52 аудиторных часов, 56 часов самостоятельной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИ О
Курс 4, Семестр 8					
Модуль 1. Понятие о DLP-системах (10 лек +18 лр + 28 ср) часов					
1.1	Лекция 1. Общие понятия о DLP-системах Утечки информации – виды, источники, методы борьбы с утечками. Концепции DLP-систем Трансформация изначальной концепции DLP Логика работы с DLP-системой. Пути развития DLP-систем	Лек	2	ПК-3	Л1.1 Л1.2 Л2.1 Л2.2 Л2.4
1.2	Лекция 2. Место DLP среди других решений на рынке. Отечественные разработки DLP	Лек	2	ПК-3	Л2.1 Л2.2 Л2.4
1.3	Лекция 3. Движение информации в DLP. Различные виды поиска в DLP-системах	Лек	2	ПК-3	Л2.1 Л2.2 Л2.4 Л3.2
1.4	Лекция 4. «Ромашка» КИБ. Описание модулей	Лек	2	ПК-3	Л1.1 Л1.2 Л2.3
1.5	Лекция 5. Профайлинг. Методы, инструменты. Преимущества КИБ	Лек	2	ПК-3	Л1.1 Л1.2
1.6	Лабораторная работа 1 Основные компоненты программного комплекса «СёрчИнформ КИБ»	ЛР	4	ПК-3	Л3.1 Л3.2
1.7	Лабораторная работа 2 Основные принципы и приемы использования DLP-системы для мониторинга утечек конфиденциальной информации (на примере программного комплекса «СёрчИнформ КИБ»)	ЛР	6	ПК-3	Л3.1 Л3.2
1.8	Лабораторная работа 3 Осуществление контроля переписки и действий пользователей при помощи различных видов поиска (на примере программного комплекса «СёрчИнформ КИБ»)	ЛР	4	ПК-3	Л3.1 Л3.2
1.9	Лабораторная работа 4 Проведение расследований с использованием возможностей программного комплекса «СёрчИнформ КИБ»	ЛР	4	ПК-3	Л3.1 Л3.2
1.10	Защита от несанкционированного доступа к информации. Термины и Определения. Доктрина информационной безопасности Российской Федерации. Указ президента российской федерации. Об утверждении перечня сведений конфиденциального характера. Положение о лицензировании деятельности по	СРС	28	ПК-3	Л1.1 Л1.2 Л2.1 Л2.2 Л2.3 Л2.4 Л3.1 Л3.2

	технической защите конфиденциальной информации. Постановление Правительства Российской Федерации от 30 апреля 2002 г. № 290. Инструкция по защите конфиденциальной информации при работе с зарубежными партнерами. Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации. Анализ моделей нарушителя; угрозы информационно-программному обеспечению вычислительных систем и их классификация Классификация каналов утечки информации. Требования к современным DLP-системам				
Модуль 2. Функции DLP-систем. настройка DLP (8 лек + 16 лр + 28 ср) часов					
2.1	Лекция 6. Виды поиска информации	Лек	2	ПК-3	Л1.1 Л1.2 Л2.1 Л3.1
2.2	Лекция 7. "AnalyticConsole: ручной и автоматический анализ информации" Применение фильтров Формирование отчетов	Лек	2	ПК-3	Л1.1 Л1.2 Л2.1 Л3.1
2.3	Лекция 8 "AlertCenter: автоматический мониторинг информационных потоков" Создание политики	Лек	2	ПК-3	Л1.1 Л1.2 Л2.1 Л3.1
2.4	Лекция 9 "Блокировка информации в КИБ СёрчИнформ" Общий принцип блокировки в DLP-системах Блокировка: настройка правил Блокировка на уровне сети Блокировка на уровне агента Блокировка почты на уровне рабочей станции или почтового сервера (агент)	Лек	2	ПК-3	Л2.2 Л2.3 Л2.4 Л3.2
2.5	Лабораторная работа 5 Настройка правил блокировки с целью предотвращения утечки конфиденциальной информации (на примере программного комплекса «СёрчИнформ КИБ»)	ЛР	4	ПК-3	Л3.2
2.6	Лабораторная работа 6 Оперативный контроль деятельности на рабочих местах пользователей локальной сети при помощи режимов LiveView, LiveCam и LiveSound, реализуемых средствами программного комплекса «СёрчИнформ КИБ»	ЛР	6	ПК-3	Л3.2
2.7	Лабораторная работа 7 Комплексное использование компонентов программного комплекса «СёрчИнформ КИБ» для контроля движение организационно-распорядительных документов и предотвращения утечки конфиденциальной информации	ЛР	6	ПК-3	Л3.2
2.10	Поведенческий анализ. Технология анализа поведения	СРС	28	ПК-3	Л1.1

	пользователей (User Behavior Analytics, UBA) Технология цифровых отпечатков (Digital fingerprints, DiFi) сравнивает текстовые, графические и табличные документы с эталонами Технология контроля идентификаторов (IDID, ID identification) позволяет распознавать в тексте сообщений специальные идентификаторы Технология графических шаблонов. Технология позволяет контролировать передачу критичных данных в графических форматах Файловый краулер. Технология позволяет проверять все узлы корпоративной сети и составлять ее наглядную карту, после чего контролировать ресурсы сети. Технология анализа текста. Детектирование текстов, близких по смыслу с эталоном Технологии глубокого поиска. Поиск изображений, похожих на эталон. Поиск по любым аудио- или видеозаписям действий пользователя Технологии пристального наблюдения. Позволяют точно восстанавливать цепочки событий и устанавливать всех причастных к нарушениям Технология автоматического выявления и группировки неизвестных документов по новым тематикам (кластеризация) Технология машинного обучения для классификации текста на базе модуля искусственного интеллекта.				Л1.2 Л2.1 Л2.2 Л2.3 Л2.4 Л3.1 Л3.2
	Зачет			ПК-3	Л1.1 Л1.2 Л2.1 Л2.2 Л2.3 Л2.4 Л3.1 Л3.2
Итого – 108 часов					

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Рекомендуемая литература				
5.1.1. Основная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л1.1	Ю. Ю. Громов, О. Г. Иванова, К. В. Стародубов, А. А. Кадыков	Программно-аппаратные средства защиты информационных систем : учебное пособие	Тамбов : ТГТУ, 2017. — 194 с.	Э1
Л1.2	Баранова, Е. К., А.В. Бабаш	Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова,. — 3-е изд., перераб. и доп. —	Москва : РИОР : ИНФРА-М, 2024. — 336 с.	Э2
5.1.2. Дополнительная литература				
Код	Авторы,	Заглавие	Издательство, год	Кол.

	составители			
Л2.1	Шипулин, Г. Ф.	Классификация средств защиты информации. Средства защиты информации: системы управления информацией о безопасности и событиями безопасности, системы предотвращения утечек данных: учебное пособие	Москва : РТУ МИРЭА, 2025. — 111 с.	Э3
Л2.2	-	DLP — система: что это такое, как работает и как выбрать	Компания стахановец, 12 января 2024	Э4
Л2.3	Компания Стахановец	Стахановец Полный Контроль - контроль действий сотрудников	Компания Стахановец	Э5
Л2.4	Компания Solar Dozor	DLP система Solar Dozor – комплексная защита информации от утечки, мониторинг работников, контроль рабочего времени, противодействие коррупции.	Компания Solar Dozor	Э6
5.1.3. Учебно-методическое обеспечение				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л3.1	Раченко, Т. А.	Информационная безопасность : учебно-методическое пособие	Тольятти : ТГУ, 2024. — 135 с.	Э7
Л3.2	А. Рябов	Обзор DLP-системы «Контур информационной безопасности SearchInform». Часть 1 — Основные функции системы	Обзор SearchInform, 19 октября 2016	Э8
5.2. Электронные образовательные ресурсы				
Э1	https://e.lanbook.com/book/319553			
Э2	https://znanium.ru/catalog/product/2082642			
Э3	https://e.lanbook.com/book/508443			
Э4	https://stakhanovets.ru/blog/dlp-sistema-cto-eto-takoe-kak-rabotaet-i-kak-vybrat/?ysclid=lrw9rz186w607738555			
Э5	https://stakhanovets.ru/kontrol-sotrudnikov/			
Э6	https://rt-solar.ru/products/solar_dozor/?ysclid=lrw9m6zu4w322594273			
Э7	https://e.lanbook.com/book/427130			
Э8	https://www.anti-malware.ru/reviews/kib_SearchInform_part1			
5.3 Информационно-справочные системы и профессиональные базы данных				
5.3.1	Консультант Плюс – https://www.consultant.ru/			
5.3.2	Гарант – https://www.garant.ru/			
5.3.3	Научная электронная библиотека (База данных): https://www.elibrary.ru			
5.3.4	Электронный ресурс http://www.securitylab.ru/			
5.3.5	Профессиональная база данных: Федеральный портал «Российское образование»: [Электронный ресурс] – Режим доступа: http://www.edu.ru/ (открытый доступ)			
5.3.6	Профессиональная база данных: Федеральный центр информационно-образовательных ресурсов: [Электронный ресурс] – Режим доступа: http://fcior.edu.ru/ (открытый доступ)			
5.3.7	Национальный открытый университет «ИНТУИТ» - https://intuit.ru/			
5.4. Программное обеспечение. DLP-системы				
СКФ МТУСИ обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:				
П1	Гарда Предприятие			

П2	Контур информационной безопасности СёрчИнформ (СёрчИнформ КИБ)
П3	DeviceLock DLP
П4	Infowatch Traffic Monitor
П5	Safetica Protection
П6	Solar Dozor
П7	Zecurion DLP
П8	АПС Стахановец

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оснащенная интерактивной доской, проектором, ПК (ноутбуком), экраном.
6.2 МТО лабораторных работ и практических занятий	
1	Лаборатория «Программно-аппаратные средства защиты информации», укомплектованная специализированной мебелью, оснащенную программно-аппаратными комплексами защиты информации, включающими в том числе средства криптографической защиты информации,
6.3 МТО рубежных контролей, экзамена	
1	Учебные аудитории, оборудованные компьютерной техникой с возможностью выхода в локальную сеть Филиала и Интернет.
6.4 МТО самостоятельной работы обучающихся	
1	Помещение для самостоятельной работы обучающихся оснащено компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ

7. Оценочные материалы

Оценочные материалы и перечень видов оценочных средств текущего контроля и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

8. Методические рекомендации для обучающихся по освоению дисциплины

Методические рекомендации по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

9. Особенности реализации дисциплины (модуля) при обучении инвалидов и лиц с ограниченными возможностями здоровья

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков.

Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания.

Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.).

Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь.

Текущий контроль успеваемости осуществляется в устной форме.

При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

10. Дополнения и изменения в Рабочей программе

Лист актуализации рабочей программы дисциплины «Б1.В.07 Аналитика DLP-систем» для использования в 20__/20__ учебном году

Утверждаю

Зам. директора по УР _____
«__» _____ 20__ г.

Направление: 10.03.01 Информационная безопасность

Профиль: Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Форма обучения: очная

(Возможны следующие варианты):

а) Рабочая программа действует без изменений.

б) В рабочую программу вносятся следующие изменения:

- 1)
- 2)
- 3)

Разработчик (и): _____
(ФИО, ученая степень, ученое звание)

«__» _____ 20__ г.

Рабочая программа пересмотрена и одобрена на заседании кафедры ИБ

Протокол № _____ от «__» _____ 20__ г.

Заведующий кафедрой _____

Оценочные материалы для проведения текущего контроля и промежуточной аттестации по дисциплине

1. Оценочные материалы для проведения промежуточной аттестации по дисциплине

1.1 Шкала оценивания компетенций

Шкала оценивания компетенций		
Оценка	Уровень освоения компетенции	Критерии оценивания
«Отлично»	Высокий уровень	Обучающийся показывает всестороннее, систематическое и глубокое знание основного и дополнительного учебного материала, умеет свободно выполнять задания, предусмотренные программой; усвоил основную и знаком с дополнительной рекомендованной литературой; может объяснить взаимосвязь основных понятий дисциплины в их значении для последующей профессиональной деятельности; проявляет творческие способности в понимании, изложении и использовании учебного материала.
«Хорошо»	Повышенный уровень	Обучающийся показывает достаточный уровень знаний в пределах основного учебного материала, без существенных ошибок выполняет предусмотренные в программе задания; усвоил основную литературу, рекомендованную в программе; способен объяснить взаимосвязь основных понятий дисциплины при дополнительных вопросах преподавателя. Допускает не существенные погрешности в ответах, устраняет их без помощи преподавателя.
«Удовлетворительно»	Пороговый уровень	Обучающийся показывает знания основного учебного материала в минимальном объеме, необходимом для дальнейшей учебы; справляется с выполнением заданий, предусмотренных программой, допуская при этом большое количество не принципиальных ошибок; знаком с основной литературой, рекомендованной программой. Допускает существенные погрешности в ответах, но обладает необходимыми знаниями для их устранения под руководством преподавателя.
«Неудовлетворительно»	Минимальный уровень не достигнут	Обучающийся обнаруживает пробелы в знаниях основного учебного материала, допускает принципиальные ошибки в выполнении предусмотренных программой заданий, не знаком с рекомендованной литературой, не может исправить допущенные ошибки. Как правило, оценка «неудовлетворительно» ставится обучающимся, которые не могут

		продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.
--	--	--

1.2 Показатели, критерии и шкалы оценивания компетенций

Показатели компетенции	Критерии оценивания	Шкала оценивания
ПК-3: Администрирование средств защиты информации прикладного и системного программного обеспечения		
Знать:		
- Архитектуру DLP-систем; - Принципы построения DLP-систем; - Основные средства и методы анализа работы программного комплекса DLP; - Источники угроз информационной безопасности, вызывающие утечку информации; - Характерные признаки наличия утечки информации; - Средства и методы обнаружения ранее источников утечки информации.	Контрольная работа 1	Модуль 1 0÷10 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-5 «Хорошо» - 6-8 «Отлично» - 9-10
	Контрольная работа 2	Модуль 2 0÷14 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-6 «Хорошо» - 7-10 «Отлично» - 11-14
Уметь		
Анализировать источники утечки информации; - Формулировать правила безопасной эксплуатации программного обеспечения; -Использовать программное обеспечение с целью определения возможного вредоносного воздействия; - Инсталлировать и эксплуатировать DLP-системы; - Осуществлять мероприятия по противодействию утечке информации с помощью DLP.	Лабораторная работа 1-4	Модуль 1 0÷10 за каждую ЛР Общая сумма баллов за 4 ЛР 40 баллов «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-5 «Хорошо» - 6-8 «Отлично» - 9-10
	Лабораторная работа 5-7	Модуль 2 0÷12 за каждую ЛР Общая сумма баллов за 3 ЛР 36 баллов «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5-6
Владеть		
- Определение порядка установки программного обеспечения DLP; - Определением выбора с DLP для конкретной организации; - Формулированием требований к DLP-системам; - Формулирование требований к встроенным средствам определения источников утечки	Лабораторная работа 1-4	Модуль 1 0÷10 за каждую ЛР Общая сумма баллов за 4 ЛР 40 баллов «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-5 «Хорошо» - 6-8 «Отлично» - 9-10

информации	Лабораторная работа 5-7	Модуль 2 0÷12 за каждую ЛР Общая сумма баллов за 3 ЛР 36 баллов «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5-6
	Зачет	0-100 баллов «Не зачтено» - 0-40 «Зачтено» - 41-100

1.3 Оценочные материалы: типовые контрольные задания, иные материалы

1.3.1 Оценочные средства текущего контроля для очной формы обучения

Данная дисциплина формирует у обучающегося 1 компетенцию. При выполнении обучающимся практического задания формируются одновременно умения и навыки, которые не представляется возможным разделить. Поэтому считаем, что вклад практических заданий в общую оценку умений и навыков равноценным.

Модуль 1 (50 баллов):

Модуль содержит 5 лекционных занятий и 4 лабораторных работы. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 10. За выполненные лабораторные работы обучающийся получает максимум 40 баллов. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы для контрольной работы (ПК-3):

1. Как расшифровывается аббревиатура DLP и когда впервые она начала использоваться?
2. Какие основные идеи лежат в основе концепции DLP?
3. Охарактеризуйте типы и категории нарушителей, для борьбы с которыми могут быть использованы DLP-системы?
4. Охарактеризуйте основные этапы развития и трансформации концепции DLP.
5. Какова логика работы DLP? Опишите принципы функционирования DLP-системы.
6. Охарактеризуйте новые задачи ИБ, реализация которых стала возможной в результате развития DLP.
7. Раскройте основные положения концепций People-Centric Security и Data-Centric Security.
8. Опишите отличительные особенности западных и отечественных DLP-систем.
9. В чем состоит суть концепции Money Loss Prevention?
10. Назовите основные преимущества и недостатки модели "DLP как сервис" (сопровождение систем DLP силами сторонней компании).
11. Охарактеризуйте место DLP-систем среди других решений на рынке средств обеспечения ИБ.
12. Опишите перспективы развития DLP.
13. Какие продукты входят в портфель разработок СёрчИнформ? Для чего они предназначены?
14. Опишите последовательность движения информации в DLP-системе.
15. Какие виды перехвата используются в современных DLP-системах?
16. Каковы особенности архитектуры "КИБ SearchInform"?
17. Перечислите основные модули/продукты, входящие в состав "КИБ SearchInform".

18. Охарактеризуйте назначение и основные возможности MailController.
19. Охарактеризуйте назначение и основные возможности IMController.
20. Охарактеризуйте назначение и основные возможности HTTPController.
21. Охарактеризуйте назначение и основные возможности DeviceController.
22. Охарактеризуйте назначение и основные возможности FTPController.
23. Охарактеризуйте назначение и основные возможности PrintController.
24. Охарактеризуйте назначение и основные возможности MicrophoneController.
25. Охарактеризуйте назначение и основные возможности MonitorController.
26. Охарактеризуйте назначение и основные возможности CameraController.
27. Охарактеризуйте назначение и основные возможности Keylogger.
28. Охарактеризуйте назначение и основные возможности CloudController.
29. Охарактеризуйте назначение и основные возможности ProgramController.
30. Охарактеризуйте назначение и основные возможности IWSController.
31. Каковы назначение и особенности использования в КИБ технологии профайлинга?
32. Назовите основные преимущества КИБ перед другими DLP-системами.
33. Какие три вида анализа информации реализованы в "КИБ SearchInform"? Для чего они предназначены?
34. Как связаны между собой эффективность поиска и смысловое соответствие результатов поисковому запросу?
35. В каких случаях целесообразно использовать фразовый поиск? Опишите особенности возможности фразового поиска в "КИБ SearchInform".
36. Что дает поиск по списку слов из DataCenter?
37. Опишите основные преимущества поиска по комбинации фраз.
38. Для чего предназначен поиск по последовательности символов?
39. Охарактеризуйте особенности поиска по номеру телефона.
40. Для чего предназначен поиск по словарю?.
41. Опишите область применения редактора словарей.
42. Опишите возможности применения синонимов при использовании фразового поиска и поиска по словарю.
43. Для каких двух задач целесообразно использовать поиск похожих? Опишите соответствующие алгоритмы.
44. Какую роль в формировании политик ИБ играет поиск по атрибутам? Какие атрибуты документов можно использовать в качестве содержания поисковых запросов?
45. В каких случаях целесообразно использовать поиск нераспознанных?
46. Какой вид поиска позволяет искать структурированную информацию, которая формируется по заданным правилам? Опишите особенности его применения?
47. В каких случаях оказывается эффективным поиск по цифровым отпечаткам? Каковы особенности его применения?
48. Как осуществляется формирование сложных запросов? В чем преимущество использования шаблонов?
49. Назовите основные правила учета ресурсоемкости различных видов поиска при формировании сложного запроса.
50. Каковы особенности применения поиска по базам данных?
51. Какую информацию позволяют получать статистические запросы?
52. В чем особенности использования поиска по формам?

Лабораторная работа №1

Основные компоненты программного комплекса «СёрчИнформ КИБ»

Контрольные вопросы ЛР№1 (ПК-3):

1. Опишите последовательность движения информации в DLP-системе.
2. Какие виды перехвата используются в современных DLP-системах?

3. Каковы особенности архитектуры «Сёрчинформ КИБ»?
4. Перечислите основные модули, входящие в состав «Сёрчинформ КИБ».
5. По каким схемам можно включить программный комплекс «Сёрчинформ КИБ» в сеть предприятия?
6. Требуется ли системный администратор в штате службы информационной безопасности и если да, то почему?
7. Перечислите основные аппаратные требования для штатного функционирования операционной системы Windows Server 2012.
8. Как установить пароль для пользователя «Администратор» Windows Server 2012?
9. Как изменить параметры учетной записи в Windows Server 2012?
10. Как разграничить права доступа в «Сёрчинформ КИБ»?
11. Назовите основные преимущества «Сёрчинформ КИБ» перед другими DLP-системами.

Лабораторная работа №2

Основные принципы и приемы использования DLP-системы для мониторинга утечек конфиденциальной информации (на примере программного комплекса «СёрчИнформ КИБ»)

Контрольные вопросы ЛР№2 (ПК-3):

1. Каково назначение AlertCenter?
 2. Какие логические блоки можно выделить в интерфейсе AlertCenter?
 3. Что представляет собой политика, формируемая при помощи средств AlertCenter?
- Охарактеризуйте основные сценарии использования политик?
4. Какую роль в создании политики играют поисковые запросы?
 5. Какая информация указывается в блоке «Перечень проверки» при формировании политики?
 6. Какие настройки необходимо осуществить, чтобы сотрудники службы ИБ смогли получать уведомления об инцидентах?
 7. Где задается периодичность проверки по заданной политике?
 8. Какую роль при создании политики играют списки исключений? Какие бывают списки?
 9. Какой инструмент может быть использован для дополнительной группировки инцидентов и документов? Перечислите его основные преимущества.
 10. Можно ли ставить на инцидент несколько меток? Что это дает?
 11. Перечислите основные сценарии использования шаблонов? Каким образом они создаются?
 12. Для чего нужна пакетная настройка политик?

Лабораторная работа №3

Осуществление контроля переписки и действий пользователей при помощи различных видов поиска (на примере программного комплекса «СёрчИнформ КИБ»)

Контрольные вопросы ЛР№3 (ПК-3):

1. Какие основные задачи позволяет решать AnalyticConsole?
2. В каких случаях на вкладке «Поиск» целесообразно использовать блок «источники данных», а в каких – сформировать группы?
3. Какие виды поиска доступны в блоке «текстовые фильтры»?
4. В каких случаях целесообразно использовать фразовый поиск? Опишите особенности применения фразового поиска в «Сёрчинформ КИБ».
5. Опишите основные преимущества поиска по комбинации фраз.
6. Для чего предназначен поиск по последовательности символов?
7. Охарактеризуйте особенности поиска по номеру телефона.
8. Для чего предназначен поиск по словарю?

9. Для каких двух задач целесообразно использовать поиск похожих? Опишите соответствующие алгоритмы.
10. Какую роль играет поиск по атрибутам? Какие атрибуты документов можно использовать в качестве содержания поисковых запросов?
11. По каким условиям могут объединяться значения простых, текстовых и фильтров по атрибутам?
12. Какую информацию содержит блок выдачи результатов на вкладке «Поиск»?
13. Меняется ли набор столбцов в блоке выдачи результатов в зависимости от канала перехвата? Если да, то почему?
14. В чем разница между вкладками «Атрибуты», «Только текст» и «Родной формат» блока предпросмотра? Каковы сценарии их использования?
15. Как осуществляется экспорт поисковой выдачи? Опишите особенности экспорта перехвата аудио\видео.

Лабораторная работа №4

Проведение расследований с использованием возможностей программного комплекса «СёрчИнформ КИБ»

1. Какую роль играет проведение расследований в обеспечении ИБ (и, в частности, в управлении инцидентами)?
2. Дайте определение понятиям «событие» и «инцидент» ИБ.
3. Приведите примеры классификаций событий и инцидентов ИБ.
4. Какие средства для проведения расследований предоставляет работникам службы ИБ программный комплекс «Сёрчинформ КИБ»?
5. Каким образом осуществляется комплексное использование различных компонентов программного комплекса «Сёрчинформ КИБ» в процессе проведения расследований? Приведите примеры.
6. Какие преимущества дает использование DLP-системы при проведении расследования инцидентов ИБ?

Модуль 2: (50 баллов):

Модуль содержит 4 лекционных занятия и 3 лабораторных работы. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 14. За выполненные и защищенные лабораторные работы обучающийся получает максимум 36 баллов. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы для контрольной работы (ПК-3):

1. Какие основные задачи позволяет решать AnalyticConsole?
2. Какие вкладки содержит AnalyticConsole? Какого рода информация содержится в каждой из них?
3. В каких случаях на вкладке "Поиск" целесообразно использовать блок "источники данных", а в каких - сформировать группы?
4. Для чего предназначены простые фильтры на вкладке "Поиск"?
5. Какие виды поиска доступны в блоке "текстовые фильтры"?
6. По каким условиям могут объединяться значения простых, текстовых и фильтров по атрибутам?
7. Какую информацию содержит блок выдачи результатов на вкладке "Поиск"?
8. Каким способом можно организовывать цепочки условий в поле для группировки?
9. Меняется ли набор столбцов в блоке выдачи результатов в зависимости от канала перехвата? Если да, то почему?.

10. В чем разница между вкладками «Атрибуты», «Только текст» и «Родной формат» блока предпросмотра? Каковы сценарии их использования?
11. Как осуществляется экспорт поисковой выдачи? Опишите особенности экспорта перехвата аудио\видео.
12. Какие задачи позволяет решить построение контентных маршрутов? Как можно построить контентный маршрут?
13. Каково содержимое вкладки "Текущая активность"?
14. Каковы особенности отображения онлайн активности пользователей на вкладке "Текущая активность"?
15. На основе какой информации формируются отчеты на одноименной вкладке?
16. Можно ли создавать собственные отчеты? Какие средства необходимо для этого использовать?
17. Перечислите и охарактеризуйте состав основных групп отчетов.
18. Каковы особенности построения отчета по связям пользователей?
19. Как определяется принадлежность аккаунтов пользователю при построении отчета «Адреса пользователей»?
20. Какого рода информацию предоставляют отчеты по Programs?
21. Как настраиваются правила продуктивностей?
22. Каким образом рассчитывается коэффициент активности? Приведите пример.
23. Каково назначение отчетов по AlertCenter?
24. Каково назначение отчетов по программам?
25. Какие события/данные фиксируют отчеты по устройствам?
26. Какую помощь службе ИБ могут оказать системные отчеты?
27. Для чего предназначены отчеты по авторизациям?
28. Какая идеология лежит в основе формирования карточек пользователей?
29. Какие подвкладки содержит вкладка "Карточки пользователей"? Опишите назначение каждой из них?
30. Охарактеризуйте информацию, размещаемую на подвкладке "Профайл" карточки пользователя.
31. Какую роль профайлинг может играть в деятельности работника службы ИБ?
32. Какую информацию включает формируемый профиль пользователя?
33. Для чего предназначена вкладка "Карантин"?
34. Как работают политики карантина?
35. Назовите основные особенности создания и использования политик карантина.
36. Как много поисковых запросов может включать критерий поиска?
37. Как осуществляются экспорт сообщений, политик и критериев карантина?
38. Какую роль в использовании политик и критериев карантина играет библиотека запросов в настройках Консоли аналитика?
39. Какие возможности работнику службы ИБ предоставляет вкладка "Task Management"?
40. Опишите особенности создания, просмотра и редактирования задач Task Management.
41. Каково назначение AlertCenter?
42. Какие логические блоки можно выделить в интерфейсе AlertCenter?
43. Что представляет собой политика, формируемая при помощи средств AlertCenter? Охарактеризуйте основные сценарии использования политик?
44. Какую роль в создании политики играют поисковые запросы?
45. Какая информация указывается в блоке «Перечень проверки» при формировании политики?
46. Какие настройки необходимо осуществить, чтобы сотрудники службы ИБ могли получать уведомления об инцидентах?
47. Где задается периодичность проверки по заданной политике?

48. Какую роль при создании политики играют списки исключений? Какие бывают списки?
49. Какой инструмент может быть использован для дополнительной группировки инцидентов и документов? Перечислите его основные преимущества.
50. Можно ли ставить на инцидент несколько меток? Что это дает?
51. Перечислите основные сценарии использования шаблонов? Каким образом они создаются?
52. Для чего нужна пакетная настройка политик?
53. Можно ли при использовании пакетной настройки политик менять расписание проверки и получателей уведомлений не только по группам политик, но и по каждой политике в отдельности?
54. Как, используя пакетную настройку политик, в почтовом клиенте организовать автоматическую сортировку писем с инцидентами?
55. Можно ли при пакетной настройке политик использовать списки исключений?
56. Для чего предназначена подкладка «Запуск внешнего скрипта» при пакетной настройке политик?
57. Каковы особенности и преимущества использования атрибутов инцидентов AlertCenter в программном продукте IRP R-Vision?
58. Какой цели служит функция блокирования передачи информации по различным каналам коммуникации в КИБ?
59. Опишите основные принципы реализации блокировок передачи информации в DLP-системах.
60. Назовите плюсы и минусы различных подходов к реализации блокировок передачи информации в DLP-системах.
61. В чем отличие блокировки по контенту от блокировки по контексту?
62. В каком приложении КИБ осуществляется настройка правил блокировки?
63. Какие элементы передаваемой информации используются для обнаружения информации с целью последующей блокировки?
64. Какие операции с файлами не осуществляются без обработки правилами блокировки?
65. Какие элементы интерфейса Endpoint Controller Console предназначены для управления правилами блокировки?
66. Опишите группы настроек, которые обеспечивают возможность добавление правила доступа к файлам соответствующего типа.
67. Какие особенности межпроцессного взаимодействия следует учитывать при настройке правила блокировки?
68. Опишите алгоритм создания правила блокировки в группе настроек "Файлы по классификации (FileAuditor)".
69. Опишите алгоритм создания правила блокировки в группе настроек "Мессенджеры (DLP)".
70. Опишите алгоритм создания правила блокировки в группе настроек "Печать по контенту (DLP)".
71. Опишите алгоритм создания правила блокировки в группе настроек "Сайты по контенту (DLP)".
72. Какую роль в процессе настройки правила блокировки в группе "Файлы по классификации (FileAuditor)" играют метки?
73. Какие именно приложения используются в качестве объектов блокировки при настройке правила в группе "Мессенджеры (DLP)"?
74. Можно ли (и если да, то каким образом) отправлять пользователю сообщения о блокировке при наличии с его стороны запроса доступа к устройствам печати?
75. Какова специфика настройки правил блокировки данных/файлов, отправляемых пользователем на те или иные веб-ресурсы?

76. Какой/какие модули перехвата должны быть активированы для блокировки веб-сайтов?
77. Где и как настраивается блокировка сетевого трафика HTTP(S)?
78. Какого рода блокировку можно настроить в модуле KeyLogger?
79. Какие действия пользователя можно заблокировать, используя настройки модуля HTTPController?
80. Какова специфика блокировок, реализуемых в модуле DeviceController?
81. Какие средства и применительно к каким каналам могут быть использованы для повышения точности блокировок в модуле DeviceController?
82. Можно ли учитывать блокировки при настройке списков исключений в модуле DeviceController?
83. Какова специфика блокировок в RDP-сессиях?
84. Какие возможности для ограничения передачи данных предоставляет группа настроек "Блокировка процессов"?
85. Что можно блокировать при помощи группы настроек "Буфер обмена"?
86. Какова специфика блокировок переносных устройств (смартфонов)?
87. Как настраивается блокировка доступа к папкам и дискам?
88. Является ли "Ограничение записи" блокировкой по контенту либо по контексту?
89. Какой принцип блокировки сетевых устройств реализуется в группе настроек "Ограничение по LAN"?
90. Что дает блокировка записи на USB?
91. Какие виды поиска можно использовать при настройке правил блокировки записи на USB?
92. В чем различие использования блокировки почты на уровне рабочей станции и почтового сервера?

Лабораторная работа №5

Настройка правил блокировки с целью предотвращения утечки конфиденциальной информации (на примере программного комплекса «СёрчИнформ КИБ»)

Контрольные вопросы ЛР№5 (ПК-3):

1. Какой цели служит функция блокирования передачи информации по различным каналам коммуникации в КИБ?
2. Опишите основные принципы реализации блокировок передачи информации в DLP-системах.
3. Назовите плюсы и минусы различных подходов к реализации блокировок передачи информации в DLP-системах.
4. Какие элементы интерфейса Endpoint Controller Console предназначены для управления правилами блокировки?
5. Опишите группы настроек, которые обеспечивают возможность добавление правила доступа к файлам соответствующего типа.
6. Можно ли (и если да, то каким образом) отправлять пользователю сообщения о блокировке при наличии с его стороны запроса доступа к устройствам печати?
7. Какой/какие модули перехвата должны быть активированы для блокировки веб-сайтов?
8. Какого рода блокировку можно настроить в модуле KeyLogger?
9. Какие действия пользователя можно заблокировать, используя настройки модуля HTTPController?
10. Какова специфика блокировок, реализуемых в модуле DeviceController?
11. Какие средства и применительно к каким каналам могут быть использованы для повышения точности блокировок в модуле DeviceController?
12. Какие возможности для ограничения передачи данных предоставляет группа настроек "Блокировка процессов"?

13. Как настраивается блокировка доступа к папкам и дискам?
14. Что дает блокировка записи на USB?

Лабораторная работа №6

Оперативный контроль деятельности на рабочих местах пользователей локальной сети при помощи режимов LiveView, LiveCam и LiveSound, реализуемых средствами программного комплекса «СёрчИнформ КИБ»

Контрольные вопросы ЛР№6 (ПК-3):

1. Какие основные функции в составе программного комплекса «СёрчИнформ КИБ» реализует платформа EndpointController?
2. Перечислите плюсы и минусы агентского перехвата.
3. Каково назначение приложения EndpointController Console?
4. Опишите основные элементы интерфейса вкладки «Сетевое окружение» приложения EndpointController Console.
5. Каким образом осуществляется инсталляция и настройка агента?
6. Какие возможности по управлению агентом представлены на вкладке «Сетевое окружение»?
7. Какое приложение в составе программного комплекса «СёрчИнформ КИБ» позволяет просматривать информацию об активности сотрудников в режиме реального времени?
8. Каковы особенности отображения онлайн активности пользователей?
9. Какое максимальное число пользователей можно одновременно отслеживать в режиме оперативного контроля?
10. Какие задачи, связанные с обеспечением информационной безопасности, можно решать, используя режимы LiveView, LiveCam и LiveSound?

Лабораторная работа №7

Комплексное использование компонентов программного комплекса «СёрчИнформ КИБ» для контроля движение организационно-распорядительных документов и предотвращения утечки конфиденциальной информации

Контрольные вопросы ЛР№7 (ПК-3):

1. Почему важно контролировать движение организационно-распорядительных документов в организации?
2. В чем смысл поправок к Федеральному закону от 27 июля 2010 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»?
3. Что представляет собой политика, формируемая при помощи средств AlertCenter?
4. Какую роль в создании политики играют поисковые запросы?
5. Как осуществляется формирование сложных запросов?
6. Опишите особенности использования фразового поиска, поиска похожих и поиска по атрибутам в составе сложного запроса.
7. Охарактеризуйте назначение и основные возможности модулей перехвата IMController и Keylogger.
8. Какую информацию содержит блок выдачи результатов на вкладке «Поиск» приложения AnalyticConsole?
9. В чем разница между вкладками «Атрибуты», «Только текст» и «Родной формат» блока предпросмотра? Каковы сценарии их использования?
10. Какой цели служит функция блокирования передачи информации по различным каналам коммуникации в КИБ?
11. Какие элементы интерфейса Endpoint Controller Console предназначены для управления правилами блокировки?
12. Какие именно приложения используются в качестве объектов блокировки при настройке правила в группе «Мессенджеры (DLP)»?
13. Какой/какие модули перехвата должны быть активированы для блокировки передачи

файлов в чатах мессенджеров?

14. Какую роль в процессе настройки правила блокировки играют метки?

15. Опишите группы настроек, которые обеспечивают возможность добавление правила доступа к файлам соответствующего типа.

1.3.2 Вопросы, выносимые на зачет по дисциплине «Аналитика DLP-систем» (ПК-3) (промежуточная аттестация):

1. Как расшифровывается аббревиатура DLP и когда впервые она начала использоваться?

2. Какие основные идеи лежат в основе концепции DLP?

3. Охарактеризуйте типы и категории нарушителей, для борьбы с которыми могут быть использованы DLP-системы?

4. Охарактеризуйте основные этапы развития и трансформации концепции DLP.

5. Какова логика работы DLP? Опишите принципы функционирования DLP-системы.

6. Охарактеризуйте новые задачи ИБ, реализация которых стала возможной в результате развития DLP.

7. Раскройте основные положения концепций People-Centric Security и Data-Centric Security.

8. Опишите отличительные особенности западных и отечественных DLP-систем.

9. В чем состоит суть концепции Money Loss Prevention?

10. Назовите основные преимущества и недостатки модели "DLP как сервис" (сопровождение систем DLP силами сторонней компании).

11. Охарактеризуйте место DLP-систем среди других решений на рынке средств обеспечения ИБ.

12. Опишите перспективы развития DLP.

13. Вопросы для самоконтроля. Модуль 2 "КИБ СёрчИнформ"

14. Какие продукты входят в портфель разработок СёрчИнформ? Для чего они предназначены?

15. Опишите последовательность движения информации в DLP-системе.

16. Какие виды перехвата используются в современных DLP-системах?

17. Каковы особенности архитектуры "КИБ SearchInform"?

18. Перечислите основные модули/продукты, входящие в состав "КИБ SearchInform".

19. Охарактеризуйте назначение и основные возможности MailController.

20. Охарактеризуйте назначение и основные возможности IMController.

21. Охарактеризуйте назначение и основные возможности HTTPController.

22. Охарактеризуйте назначение и основные возможности DeviceController.

23. Охарактеризуйте назначение и основные возможности FTPController.

24. Охарактеризуйте назначение и основные возможности PrintController.

25. Охарактеризуйте назначение и основные возможности MicrophoneController.

26. Охарактеризуйте назначение и основные возможности MonitorController.

27. Охарактеризуйте назначение и основные возможности CameraController.

28. Охарактеризуйте назначение и основные возможности Keylogger.

29. Охарактеризуйте назначение и основные возможности CloudController.

30. Охарактеризуйте назначение и основные возможности ProgramController.

31. Охарактеризуйте назначение и основные возможности IWSController.

32. Каковы назначение и особенности использования в КИБ технологии профайлинга?

33. Назовите основные преимущества КИБ перед другими DLP-системами.

34. Вопросы для самоконтроля. Модуль 3 "Виды поиска"

35. Какие три вида анализа информации реализованы в "КИБ SearchInform"? Для чего

они предназначены?

36. Как связаны между собой эффективность поиска и смысловое соответствие результатов поисковому запросу?

37. В каких случаях целесообразно использовать фразовый поиск? Опишите особенности возможности фразового поиска в "КИБ SearchInform".

38. Что дает поиск по списку слов из DataCenter?

39. Опишите основные преимущества поиска по комбинации фраз.

40. Для чего предназначен поиск по последовательности символов?

41. Охарактеризуйте особенности поиска по номеру телефона.

42. Для чего предназначен поиск по словарю?.

43. Опишите область применения редактора словарей.

44. Опишите возможности применения синонимов при использовании фразового поиска и поиска по словарю.

45. Для каких двух задач целесообразно использовать поиск похожих? Опишите соответствующие алгоритмы.

46. Какую роль в формировании политик ИБ играет поиск по атрибутам? Какие атрибуты документов можно использовать в качестве содержания поисковых запросов?

47. В каких случаях целесообразно использовать поиск нераспознанных?

48. Какой вид поиска позволяет искать структурированную информацию, которая формируется по заданным правилам? Опишите особенности его применения?

49. В каких случаях оказывается эффективным поиск по цифровым отпечаткам? Каковы особенности его применения?

50. Как осуществляется формирование сложных запросов? В чем преимущество использования шаблонов?

51. Назовите основные правила учета ресурсоемкости различных видов поиска при формировании сложного запроса.

52. Каковы особенности применения поиска по базам данных?

53. Какую информацию позволяют получать статистические запросы?

54. В чем особенности использования поиска по формам?

55. Вопросы для самоконтроля. Модуль 4 "AnalyticConsole: ручной и автоматический анализ информации"

56. Какие основные задачи позволяет решать AnalyticConsole?

57. Какие вкладки содержит AnalyticConsole? Какого рода информация содержится в каждой из них?

58. В каких случаях на вкладке "Поиск" целесообразно использовать блок "источники данных", а в каких - сформировать группы?

59. Для чего предназначены простые фильтры на вкладке "Поиск"?

60. Какие виды поиска доступны в блоке "текстовые фильтры"?

61. По каким условиям могут объединяться значения простых, текстовых и фильтров по атрибутам?

62. Какую информацию содержит блок выдачи результатов на вкладке "Поиск"?

63. Каким способом можно организовывать цепочки условий в поле для группировки?

64. Меняется ли набор столбцов в блоке выдачи результатов в зависимости от канала перехвата? Если да, то почему?.

65. В чем разница между вкладками «Атрибуты», «Только текст» и «Родной формат» блока предпросмотра? Каковы сценарии их использования?

66. Как осуществляется экспорт поисковой выдачи? Опишите особенности экспорта перехвата аудио\видео.

67. Какие задачи позволяет решить построение контентных маршрутов? Как можно построить контентный маршрут?

68. Каково содержимое вкладки "Текущая активность"?

69. Каковы особенности отображения онлайн активности пользователей на вкладке

"Текущая активность"?

70. На основе какой информации формируются отчеты на одноименной вкладке?

71. Можно ли создавать собственные отчеты? Какие средства необходимо для этого использовать?

72. Перечислите и охарактеризуйте состав основных групп отчетов.

73. Каковы особенности построения отчета по связям пользователей?

74. Как определяется принадлежность аккаунтов пользователю при построении отчета «Адреса пользователей»?

75. Какого рода информацию предоставляют отчеты по Programs?

76. Как настраиваются правила продуктивностей?

77. Каким образом рассчитывается коэффициент активности? Приведите пример.

78. Каково назначение отчетов по AlertCenter?

79. Каково назначение отчетов по программам?

80. Какие события/данные фиксируют отчеты по устройствам?

81. Какую помощь службе ИБ могут оказать системные отчеты?

82. Для чего предназначены отчеты по авторизациям?

83. Какая идеология лежит в основе формирования карточек пользователей?

84. Какие подвкладки содержит вкладка "Карточки пользователей"? Опишите назначение каждой из них?

85. Охарактеризуйте информацию, размещаемую на подвкладке "Профайл" карточки пользователя.

86. Какую роль профайлинг может играть в деятельности работника службы ИБ?

87. Какую информацию включает формируемый профиль пользователя?

88. Для чего предназначена вкладка "Карантин"?

89. Как работают политики карантина?

90. Назовите основные особенности создания и использования политик карантина.

91. Как много поисковых запросов может включать критерий поиска?

92. Как осуществляются экспорт сообщений, политик и критериев карантина?

93. Какую роль в использовании политик и критериев карантина играет библиотека запросов в настройках Консоли аналитика?

94. Какие возможности работнику службы ИБ предоставляет вкладка "Task Management"?

95. Опишите особенности создания, просмотра и редактирования задач Task Management.

96. Вопросы для самоконтроля. Модуль 5 "AlertCenter: автоматический мониторинг информационных потоков"

97. Каково назначение AlertCenter?

98. Какие логические блоки можно выделить в интерфейсе AlertCenter?

99. Что представляет собой политика, формируемая при помощи средств AlertCenter?

Охарактеризуйте основные сценарии использования политик?

100. Какую роль в создании политики играют поисковые запросы?

101. Какая информация указывается в блоке «Перечень проверки» при формировании политики?

102. Какие настройки необходимо осуществить, чтобы сотрудники службы ИБ смогли получать уведомления об инцидентах?

103. Где задается периодичность проверки по заданной политике?

104. Какую роль при создании политики играют списки исключений? Какие бывают списки?

105. Какой инструмент может быть использован для дополнительной группировки инцидентов и документов? Перечислите его основные преимущества.

106. Можно ли ставить на инцидент несколько меток? Что это дает?

107. Перечислите основные сценарии использования шаблонов? Каким образом они

создаются?

108.Для чего нужна пакетная настройка политик?

109.Можно ли при использовании пакетной настройки политик менять расписание проверки и получателей уведомлений не только по группам политик, но и по каждой политике в отдельности?

110.Как, используя пакетную настройку политик, в почтовом клиенте организовать автоматическую сортировку писем с инцидентами?

111.Можно ли при пакетной настройке политик использовать списки исключений?

112.Для чего предназначена подкладка «Запуск внешнего скрипта» при пакетной настройке политик?

113.Каковы особенности и преимущества использования атрибутов инцидентов AlertCenter в программном продукте IRP R-Vision?

114.Вопросы для самоконтроля. Модуль 6 "Блокировка информации в КИБ СёрчИнформ"

115.Какой цели служит функция блокирования передачи информации по различным каналам коммуникации в КИБ?

116.Опишите основные принципы реализации блокировок передачи информации в DLP-системах.

117.Назовите плюсы и минусы различных подходов к реализации блокировок передачи информации в DLP-системах.

118.В чем отличие блокировки по контенту от блокировки по контексту?

119.В каком приложении КИБ осуществляется настройка правил блокировки?

120.Какие элементы передаваемой информации используются для обнаружения информации с целью последующей блокировки?

121.Какие операции с файлами не осуществляются без обработки правилами блокировки?

122.Какие элементы интерфейса Endpoint Controller Console предназначены для управления правилами блокировки?

123.Опишите группы настроек, которые обеспечивают возможность добавление правила доступа к файлам соответствующего типа.

124.Какие особенности межпроцессного взаимодействия следует учитывать при настройке правила блокировки?

125.Опишите алгоритм создания правила блокировки в группе настроек "Файлы по классификации (FileAuditor)".

126.Опишите алгоритм создания правила блокировки в группе настроек "Мессенджеры (DLP)".

127.Опишите алгоритм создания правила блокировки в группе настроек "Печать по контенту (DLP)".

128.Опишите алгоритм создания правила блокировки в группе настроек "Сайты по контенту (DLP)".

129.Какую роль в процессе настройки правила блокировки в группе "Файлы по классификации (FileAuditor)" играют метки?

130.Какие именно приложения используются в качестве объектов блокировки при настройке правила в группе "Мессенджеры (DLP)"?

131.Можно ли (и если да, то каким образом) отправлять пользователю сообщения о блокировке при наличии с его стороны запроса доступа к устройствам печати?

132.Какова специфика настройки правил блокировки данных/файлов, отправляемых пользователем на те или иные веб-ресурсы?

133.Какой/какие модули перехвата должны быть активированы для блокировки веб-сайтов?

134.Где и как настраивается блокировка сетевого трафика HTTP(S)?

135.Какого рода блокировку можно настроить в модуле KeyLogger?

- 136.Какие действия пользователя можно заблокировать, используя настройки модуля HTTPController?
- 137.Какова специфика блокировок, реализуемых в модуле DeviceController?
- 138.Какие средства и применительно к каким каналам могут быть использованы для повышения точности блокировок в модуле DeviceController?
- 139.Можно ли учитывать блокировки при настройке списков исключений в модуле DeviceController?
- 140.Какова специфика блокировок в RDP-сессиях?
- 141.Какие возможности для ограничения передачи данных предоставляет группа настроек "Блокировка процессов"?
- 142.Что можно блокировать при помощи группы настроек "Буфер обмена"?
- 143.Какова специфика блокировок переносных устройств (смартфонов)?
- 144.Как настраивается блокировка доступа к папкам и дискам?
- 145.Является ли "Ограничение записи" блокировкой по контенту либо по контексту?
- 146.Какой принцип блокировки сетевых устройств реализуется в группе настроек "Ограничение по LAN"?
- 147.Что дает блокировка записи на USB?
- 148.Какие виды поиска можно использовать при настройке правил блокировка записи на USB?
- 149.В чем различие использования блокировки почты на уровне рабочей станции и почтового сервера?
- 150.Вопросы для самоконтроля. Модуль 7 "FileAuditor СёрчИнформ: аудит операций в файловой системе и прав доступа к файлам"
- 151.Какова основная область применения решений класса DCAP?
- 152.Перечислите основные функции DCAP-систем.
- 153.Какие продукты представлены на российском рынке DCAP-систем?
- 154.Для работы с какими данными предназначен FileAuditor?
- 155.Какие задачи решает FileAuditor?
- 156.В чем заключаются основные отличия FileAuditor от ИРС?
- 157.Какова логика работы FileAuditor'a?
- 158.Где осуществляется настройка сканирования ресурсов и правил поиска конфиденциальных документов?
- 159.Как осуществляется настройка автоматической классификации данных? Опишите основные шаги.
- 160.Какой вариант поискового движка использует FileAuditor?
- 161.Какие преимущества дает использование шаблонов?
- 162.Каковы основные отличия в логике использования шаблонов сканирования в FileAuditor по сравнению с шаблонами политик в AlertCenter?
- 163.Как осуществляется настройка ручной классификации данных? Опишите основные шаги.
- 164.Опишите подробно, каким образом присваиваются файлам метки классификатора.
- 165.Как настраиваются правила автоматического управления метками?
- 166.Как производится настройка служб анализа данных на агенте и на сервере?
- 167.Есть ли возможность в процессе сканирования (если есть, то укажите каким образом) распознавать текст из графических файлов?
- 168.Распространяется ли действие правил сканирования на папки/файлы и сетевые пути, внесенные в списки исключений?
- 169.Где и как осуществляется просмотр файлов, контролируемых FileAuditor'ом?
- 170.Можно ли по данным FileAuditor'a построить контентный маршрут?
- 171.Какого рода информацию предоставляет подкладка "Отчет" на вкладке "Файловый аудитор" в Консоли аналитика?
- 172.Как лицензируется FileAuditor?

173.Вопросы для самоконтроля. Модуль 8 "Профайл центр: оценка рисков, связанных с человеческим фактором"

174.Охарактеризуйте информацию, размещаемую на вкладке "Профайл центр".

175.Какую роль профайлинг может играть в деятельности работника службы ИБ?

176.Каковы принципы, лежащие в основе реализации идей профайлинга в КИБ?

177.Опишите основные блоки информации, размещаемой в AnalyticConsole на вкладке "Профайл центр"/

178.Опишите особенности каждого из используемых в профайлинге психотипов.

179.Какую информацию включает формируемый профиль пользователя?

180.Какую роль в формировании профиля играет информация о базовых ценностях?

181.Как определяются криминальные тенденции?

182.Какими соображениями следует руководствоваться, интерпретируя уровень амбиций сотрудника?

183.Что отражает индекс личностных качеств?

184.Каким образом можно отследить динамику профиля пользователей?

185.Охарактеризуйте прикладные аспекты поиска по характеристикам пользователя.

186.Каковы особенности построения рейтингов пользователей?

187.Как настраиваются оповещения об изменениях в рейтингах?

2. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Порядок и методика проведения текущего контроля промежуточной аттестации

Предусмотрены следующие виды контроля:

- текущий контроль по каждому модулю – в форме написания контрольной работы для оценки теоретических знаний;

- текущий контроль по каждому модулю – в форме отчетов по лабораторным работам и практическим занятиям для оценки практических навыков;

- промежуточная аттестация по дисциплине – в форме зачета.

Текущий контроль успеваемости в форме защиты лабораторных и практических проводится в два этапа:

- 1-й этап: допуск к выполнению лабораторной работы – проводится в форме письменной «летучки» (5-10 мин) с целью контроля знаний обучающихся теоретической части лабораторной работы и готовности к выполнению практических исследований;

- 2-й этап выполняется по окончании каждой лабораторной работы (практического занятия) в форме индивидуального собеседования по выполненным исследованиям или расчетам. Проводится с целью контроля закрепления теоретической части материала и степени отработки обучающимся практических навыков исследования на аппаратуре.

Контрольные работы выполняются в виде короткого письменного ответа на один вопрос, изученный на предыдущей лекции в начале каждой последующей лекции. Ответ на вопрос дается в течение 5-10 минут. Таким образом, после лекционного курса каждого модуля формируется общая оценка за теоретические знания.

С целью повышения качества обучения за счет побуждения обучающихся к активной текущей учебной работе, четкого и оперативного контроля всего хода учебного процесса, снижения роли случайных и субъективных факторов при оценивании учебной деятельности обучающихся в образовательном процессе реализована модульно-рейтинговая система.

Правила ее использования прописаны в «Положении об МРС».

Набранные обучающимся баллы в рамках текущего контроля переводятся в оценку на зачете в соответствии со следующей шкалой:

- «не зачтено» - от 0 до 40 от максимального количества баллов;
- «зачтено» - от 41 до 100 максимального количества баллов.

Соотношения максимального количества баллов, полученных обучающимся по блокам модулей, показаны в Таблице .

Таблица - Распределение баллов по модулям дисциплины «Аналитика DLP-систем»

Модуль	Всего баллов (Максимальное значение)	Теоретический блок (Контрольная работа)	Практический блок
Модуль 1	50	10	40
Модуль 2	50	14	36
Зачет	100	100	

Теоретический блок оценивается по результатам контрольной работы. Практический блок оценивается по результатам выполнения лабораторных работ.

На зачете производится оценка тех компетенций, которые должны быть в той или иной форме освоены в процессе изучения. Рекомендуется формировать вопросы в билетах таким образом, чтобы преподаватель смог оценить все компетенции данной дисциплины.

3. Промежуточная аттестация

Промежуточная аттестация проводится в форме зачета. Зачет проводится по расписанию в устном виде по билетам к зачету. Результаты аттестации заносятся в ведомость и зачетную книжку обучающегося.

Образец билета к зачету

	МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»	Утверждаю Зав. кафедрой «ИБ» Жуковский А.Г. «__» ____ 20__ г.
Направление подготовки: 10.03.01 Информационная безопасность Курсы: 4 Дисциплина: Аналитика DLP-систем		
Билет №1 1. Охарактеризуйте типы и категории нарушителей, для борьбы с которыми могут быть использованы DLP-системы? 2. Каковы принципы, лежащие в основе реализации идей профайлинга в КИБ? «__» ____ 20__ г. Профессор кафедры «ИБ» _____ Жуковский А.Г.		

Один комплект отпечатанных билетов, подписанных преподавателем кафедры и утвержденных заведующим кафедрой хранится у заведующего кафедрой, другой комплект – у преподавателя, ведущего дисциплину

Вопросы для тестирования в рамках проведения внутренней независимой оценки качества образования (ПК-3)

Один комплект тестовых вопросов с указанием правильных ответов хранится у заведующего кафедрой, другой комплект – у преподавателя, ведущего дисциплину.

- 1) К правовым методам, обеспечивающим информационную безопасность, относятся:
 - Разработка аппаратных средств обеспечения правовых данных
 - Разработка и установка во всех компьютерных правовых сетях журналов учета действий
 - Разработка и конкретизация правовых нормативных актов обеспечения безопасности
- 2) Основными источниками угроз информационной безопасности являются все указанное в списке:
 - Хищение жестких дисков, подключение к сети, инсайдерство
 - Перехват данных, хищение данных, изменение архитектуры системы
 - Хищение данных, подкуп системных администраторов, нарушение регламента работы
- 3) Виды информационной безопасности:
 - Персональная, корпоративная, государственная
 - Клиентская, серверная, сетевая
 - Локальная, глобальная, смешанная
- 4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
 - несанкционированного доступа, воздействия в сети
 - инсайдерства в организации
 - чрезвычайных ситуаций
- 5) Основные объекты информационной безопасности:
 - Компьютерные сети, базы данных
 - Информационные системы, психологическое состояние пользователей
 - Бизнес-ориентированные, коммерческие системы
- 6) Основными рисками информационной безопасности являются:
 - Искажение, уменьшение объема, перекодировка информации
 - Техническое вмешательство, выведение из строя оборудования сети
 - Потеря, искажение, утечка информации
- 7) К основным принципам обеспечения информационной безопасности относятся:
 - Экономической эффективности системы безопасности
 - Многоплатформенной реализации системы
 - Усиления защищенности всех звеньев системы
- 8) Основными субъектами информационной безопасности являются:
 - руководители, менеджеры, администраторы компаний
 - органы права, государства, бизнеса
 - сетевые базы данных, файерволы
- 9) К основным функциям системы безопасности можно отнести все перечисленное:
 - Установление регламента, аудит системы, выявление рисков
 - Установка новых офисных приложений, смена хостинг-компании
 - Внедрение аутентификации, проверки контактных данных пользователей
- 10) Принципом информационной безопасности является принцип недопущения:
 - Неоправданных ограничений при работе в сети (системе)
 - Рисков безопасности сети, системы
 - Презумпции секретности
- 11) Принципом политики информационной безопасности является принцип:
 - Невозможности миновать защитные средства сети (системы)
 - Усиления основного звена сети, системы
 - Полного блокирования доступа при риск-ситуациях
- 12) Принципом политики информационной безопасности является принцип:
 - Усиления защищенности самого незащищенного звена сети (системы)
 - Перехода в безопасное состояние работы сети, системы
 - Полного доступа пользователей ко всем ресурсам сети, системы
- 13) Принципом политики информационной безопасности является принцип:
 - Разделения доступа (обязанностей, привилегий) клиентам сети (системы)

- Одноуровневой защиты сети, системы
 - Совместимых, однотипных программно-технических средств сети, системы
- 14) К основным типам средств воздействия на компьютерную сеть относится:
- Компьютерный сбой
 - Логические закладки («мины»)
 - Аварийное отключение питания
- 15) Когда получен спам по e-mail с приложенным файлом, следует:
- Прочитать приложение, если оно не содержит ничего ценного – удалить
 - Сохранить приложение в папке «Спам», выяснить затем IP-адрес генератора спама
 - Удалить письмо с приложением, не раскрывая (не читая) его
- 16) Принцип Кирхгофа:
- Секретность ключа определена секретностью открытого сообщения
 - Секретность информации определена скоростью передачи данных
 - Секретность закрытого сообщения определяется секретностью ключа
- 17) ЭЦП – это:
- Электронно-цифровой преобразователь
 - Электронно-цифровая подпись
 - Электронно-цифровой процессор
- 18) Наиболее распространены угрозы информационной безопасности корпоративной системы:
- Покупка нелегального ПО
 - Ошибки эксплуатации и неумышленного изменения режима работы системы
 - Сознательного внедрения сетевых вирусов
- 19) Наиболее распространены угрозы информационной безопасности сети:
- Распределенный доступ клиент, отказ оборудования
 - Моральный износ сети, инсайдерство
 - Сбой (отказ) оборудования, нелегальное копирование данных
- 20) Наиболее распространены средства воздействия на сеть офиса:
- Слабый трафик, информационный обман, вирусы в интернет
 - Вирусы в сети, логические мины (закладки), информационный перехват
 - Компьютерные сбои, изменение администрирования, топологии
- 21) Утечкой информации в системе называется ситуация, характеризующаяся:
- Потерей данных в системе
 - Изменением формы информации
 - Изменением содержания информации
- 22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
- Целостность
 - Доступность
 - Актуальность
- 23) Угроза информационной системе (компьютерной сети) – это:
- Вероятное событие
 - Детерминированное (всегда определенное) событие
 - Событие, происходящее периодически
- 24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
- Регламентированной
 - Правовой
 - Защищаемой
- 25) Разновидностями угроз безопасности (сети, системы) являются все перечисленные в списке:
- Программные, технические, организационные, технологические
 - Серверные, клиентские, спутниковые, наземные
 - Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:

- Владелец сети
- Администратор сети
- Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:

- Руководств, требований обеспечения необходимого уровня безопасности
- Инструкций, алгоритмов поведения пользователя в сети
- Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики безопасности является:

- Аудит, анализ затрат на проведение защитных мер
- Аудит, анализ безопасности
- Аудит, анализ уязвимостей, риск-ситуаций

29) Очень сложные пароли гарантируют 100% защиту?

А.Нет

Б.Да, если после работы полностью очищать куки и не хранить пароль на компьютере

В.Да, если пароль не сохранен на компьютере

30.Какие вирусы активизируются после включения ОС?

А.Снифферы

Б.Загрузочные

В.Трояны

Г.Черви

31.Представляют ли угрозу вирусы для крупных компаний?

А.Нет

Б.Да, представляют

В.Скорее нет. В крупных компаниях развита система безопасности

Г.Если компания обладает сотрудниками занимающимися безопасностью сети, вирусы не могут нанести такому предприятию вреда

32.С чем связана атака введением произвольных запросов в базу данных?

А.Уязвимость SQL Injection

Б.Сбой Denial of Service

В.Ошибка Denial of Service

Г.Неполадка PHP Include

33.Фильтрация контента, для чего она служит?

А.Защищает от скрытой загрузки вредоносного программного обеспечения +

Б.Помогает быстро находить в сети требуемый контент сохраняя при этом много драгоценного времени

В.Отключает назойливую рекламу

Г.Отсеивает поисковый спам

34.Какой уровень безопасности трафика обеспечивает WPA2?

А.Высокий

Б.Низкий

В.Достаточный для домашней сети

Г.Средний

35.Сколько минимально символов должен содержать безопасный пароль, состоящий из латинских строчных букв?

А.15

Б.8

В.10

Г.6

36.Какую угрозу можно назвать преднамеренной? Сотрудник:

А.Открыл письмо содержащее вредоносное ПО

Б.Ввел неправильные данные

В.Совершил не авторизованный доступ

Г.Включил компьютер без разрешения

37. Безопасно ли вводить пароли простым копированием?
А.Безопасно если это мой компьютер
Б.Да
В.Безопасно если после работы очистить куки
Г.Нет
- 38.Какую защиту необходимо использовать против программы iGIS или ее аналогов?
А.Шифровать трафик
Б.Использовать очень сложные пароли
В.Устанавливать только лицензионные антивирусы
Г.Не пользоваться Wi-fi
39. Что может привести к заражению компьютера?
А.Получение сообщения по электронной почте
Б.Загрузка пиратского ПО
В.Создание нового файла
Г.Отправка сообщения по электронной почте
40. Что такое Brute Force?
А.Взлом методом заражения системы через вредоносный файл
Б.Метод заставляющий пользователя самому раскрыть конфиденциальную информацию
В.Получение конфиденциальной информации с компьютера методом электронной рассылки
Г.Взлом методом перебора паролей
41. В каком блок файле autorun.inf чаще всего прописывается вредоносная программа?
А.Open
Б.Setup
В.Downloadе
Г.Dll
42. Как называется преднамеренно внесенный в программное обеспечение объект, приводящий к действиям программного обеспечения не предусмотренным производителем, приводящим к нарушению конфиденциальности и целостности информации?
А.Троян
Б.Бэкдор
В.Закладка
Г.Вирус
43. Безопасно ли сохранять пароли в автозаполнении браузера?
А.Да, если пароль к входу в систему знаю только я один
Б.Нет
В.Да, если этим компьютером пользуюсь только я один
Г.Да
44. Для чего служит DLP? Система выполняет функцию:
А.Защита компьютера от вирусов
Б.Выполняет функцию безопасного ввода паролей
В.Предотвращает утечку информации с компьютера
Г.Предупреждает пользователя о попытках взлома и хакерских атаках
45. Антивирус полностью защищает компьютер от вирусов и атак при работе в сети. Вы согласны с этим?
А.Нет
Б.Да, если это лицензионный антивирус известного производителя
В.Защищает совместно с включенным брандмауэром
Г.Да
46. Самый лучший способ хранения паролей в информационной системе?
А.Хеширование
Б.Вообще не сохранять
В.Архивирование
Г.Хранить только с включенным брандмауэром

47. Какое минимальное количество символов должен содержать пароль входа субъектов в систему АС, при классе защищенности 1А?
- А.12
 - Б.8
 - В.10
 - Г.15
48. На каких системах более динамично распространяются вирусы?
- А.Linux
 - Б.MacOS
 - В.Android
 - Г.Windows
49. Самая массовая угроза компьютерной безопасности, это:
- А.Спам
 - Б.Трояны
 - В.Черви
 - Г.Шпионские программы
50. Если компьютер работает в нормальном режиме, означает ли это что он не заражен?
- А.Нет
 - Б.Если не изменилась скорость работы, компьютер совершенно чист
 - В.Да
 - Г.Если антивирус ничего не показывает компьютер чист
51. Установка одновременно нескольких антивирусных программ повышает защищенность. Вы согласны с этим?
- А.Да
 - Б.Да, если это антивирусы от известных производителей
 - В.Да, если это антивирусы одного производителя
 - Г.Нет
52. Что чаще всего используют злоумышленники при атаке на компьютеры должностных лиц и руководителей крупных компаний?
- А.Фишинг
 - Б.Спам
 - В.Загрузка скрытого вредоносного ПО
 - Г.DDoS атаки
53. Как гарантировать 100% защищенность компьютера от заражения вирусами в сети?
- А.Включить брандмауэр
 - Б.Установить новое программное обеспечение
 - В.Таких гарантий нет
 - Г.Посещать только сайты известных брендов
54. Что необходимо выполнять для контроля безопасности электронной почты?
- А.Часто сменять пароли
 - Б.Проверять страницу посещения
 - В.Регистрировать почтовый ящик только в известных системах
 - Г.Использовать сложные пароли
55. Что такое Firewall, для чего он нужен?
- А.для фильтрации трафика
 - Б.для очистки компьютера
 - В.для быстрого и безопасного поиска информации
 - Г.для форматирования
56. Обеспечивает ли форматирование жесткого диска полное избавление от вирусов?
- А.Обеспечивает полностью
 - Б.Обеспечивает если выполнено быстрое форматирование
 - В.Нет
 - Г.Обеспечивает при низкоуровневом форматировании
57. Можно ли хранить важную информацию на жестком диске компьютера, в том числе пароли?

- А. Да, если это мой личный компьютер
- Б. Да
- В. Нет
- Г. Да, если компьютер не подключен к интернету

58. Если, не нажимая на иконки просто просмотреть подозрительный сайт, ничего не произойдет. Вы согласны?
А. Нет. Заражение может произойти, даже если вы просто посмотрели информацию с экрана, при этом ничего не нажимая

Б. Да, простой просмотр не наносит никакого вреда

В. Да, заражение происходит только после кликов, чем запускается вирусная программа.

59. Что такое государственная тайна?

- 1) Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ
- 2) Сведения о состоянии окружающей среды
- 3) Все сведения, которые хранятся в государственных базах данных
- 4) Сведения о состоянии здоровья президента РФ
- 5) Конкретные сведения, в отношении которых компетентные органы и их должностные лица приняли решение об их отнесении к государственной тайне

60. Что такое коммерческая тайна?

- 1) Информация, имеющая действительную или потенциальную коммерческую ценность в силу ее неизвестности третьим лицам
- 2) Информация, к которой нет доступа на законном основании
- 3) Информации, обладатель которой принимает меры к охране ее конфиденциальности
- 4) Информация, содержащая в учредительных документах
- 5) Информация, содержащая в годовых отчетах, бухгалтерских балансах, формах государственных статистических отчетов

Методика оценивания знаний

Максимальное время выполнения теста - 60 минут.

Количество вопросов в тестовом задании - 60.

Для проведения контроля знаний компьютер формирует в случайном порядке тестовые вопросы.

При прохождении тестового контроля знаний обучающийся должен выбрать один или несколько правильных ответов на один из вопросов тестового задания.

В случае правильного ответа на 49 и более тестовых вопросов (>81%) обучающийся подтверждает освоение компетенций с оценкой «отлично», при ответе на 48-37 вопросов (61-80%) обучающийся подтверждает освоение компетенций с оценкой «хорошо», при ответе на 36-25 вопросов (41-60%) обучающийся подтверждает освоение компетенций с оценкой «удовлетворительно», при ответе менее чем на 25 вопросов (<41%) обучающийся не подтверждает необходимый уровень знаний и оценивается неудовлетворительно.

4 Тестовые задания по дисциплине «Аналитика DLP-систем»

Тестовые задания позволяют оценить уровень сформированности компетенции ПК-3 - Администрирование средств защиты информации прикладного и системного программного обеспечения.

Задания распределены по блокам в соответствии с уровнем сложности. Каждый блок содержит номер задания, и текст задания.

Базовый уровень (Блок А) содержит примерно 50 % заданий.

Он формируется из заданий с выбором одного или нескольких верных ответов из предложенных или воспроизведения фактического материала (терминология, факты, классификация, параметры и др.);

Повышенный уровень (Блок Б) в среднем составляет 35 % заданий.

В нем используются задания на сопоставление, сравнение, установление последовательности;

Высокий уровень (Блок В) в среднем составляют – 15 % заданий.

В заданиях используются: решения нетиповых задач, алгоритмы, доказательства, задания с развернутым ответом – определения, перечисление, изображение схемы, структуры и др.

Количество заданий по компетенции ПК-3 равно 20.

Ключи к ответам представлены в отдельной таблице.

БЛОК А (базовый уровень) – Задание с выбором одного или нескольких верных ответов из предложенных

Инструкция по тестам Блока А: Прочитайте текст и выберите один или несколько правильных ответов

№ задания	Тексты заданий
1	Система предотвращения утечки информации обозначается как 1. IRP 2. SIEM 3. DLP 4. SOC
2	К ключевым задачам DLP, которые учитываются при настройке политик безопасности, относятся 1. Контроль за перемещением конфиденциальных документов 2. Контроль персонала 3. Поведенческий анализ 4. Оптимизация работы компании 5. Контроль действий хакеров 1,2,3,4
3	В DLP –системах используются: 1. Контроль посещения сайтов, 2. Контроль личной жизни сотрудников. 3. Поведенческий анализ сотрудников. 4. Контроль переписки сотрудников. 1,3,4
4	Российские DLP – системы в отличие от западных: 1. Имеют два режима работы – скрытый и открытый. 2. Ведут полноценный архив перехваченной информации. 3. Позволяют проводить ретроспективные расследования. 4. Имеют только открытый режим работы. 5. Не ведут полноценный архив перехваченной информации. 1,2,3
5	Развитие DLP-систем продолжается и происходит одновременно по нескольким направлениям: 1. Каналы 2. Аналитика 3. Платформы 4. UBA 5. SAMBA 1,2,3,4
6	DLP-системы поддерживают следующие ОС семейства Linux: 1. AstraLinux;

№ задания	Тексты заданий
	2. AltLinux; 3. GosLinux; 4. Rosa; 5. Kali; 6. Gentoo. 1,2,3,4
7	К категории нарушителей, для борьбы с которыми могут быть использованы DLP-системы относятся: 1. Сотрудники и руководители организации 2. Лица, имеющие с организацией активные договорные отношения 3. Киберпреступные организации 4. Конкуренты 5. Добросовестные партнеры 1,2,3,4
8	Источником информации в DLP-системах являются: 1. Серверы компании 2. Сетевые устройства 3. Рабочие станции 4. Социальные сети 3.
9	В состав DLP-системы входят следующие модули: 1. MailController 2. DeviceController 3. HTTPController 4. FTPController 5. PrintController 6. Все перечисленные
10	В DLP доступны следующие виды поиска: 1. Фразовый поиск 2. Базовый поиск 3. Поиск по словарю 4. Поиск похожих 5. Поиск по регулярным выражениям 1,3,4,5

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление соответствия
Инструкция: Прочитайте текст и установите соответствие

№ задания	Тексты заданий
11	Вся активность пользователя за компьютером перехватывается сборщиками. Понятие «сборщик» объединяет в себе несколько способов перехвата информации: 1. Сетевой перехват; 2. Перехват путем интеграции; 3. Перехват «в разрыв»; 4. Анализ данных в покое. Установите соответствие определениям каждого из способов перехвата. А. Информация никуда не передается, а хранится на винчестере или на флешке.4 Б. Позволяет блокировать любую информацию.3 В. Получение доступа к информации, передаваемой между устройствами в сетевой инфраструктуре.1 Г. Получение данных, передаваемых по техническим каналам, с помощью интеграции различных систем и инструментов.2
12	Поиск информации в DLP имеет множество опций, таких как 1. Поиск с морфологией 2. Точное совпадение 3. Начинающиеся со слов 4. Содержащие слова 5. Оканчивающиеся словами Поставьте в соответствие опций их определению А. Благодаря использованию особого аналитического блока могут быть идентифицированы все возможные словоформы. При запросе «автомобиль» производится поиск всех возможных словоформ – «автомобиль», «автомобили», «автомобилей» и т.д.1 Б. Обнаруживаются только заданные пользователем словоформы. При запросе «автомобиль»

№ задания	Тексты заданий
	будут обнаружены лишь документы, содержащие словоформу «автомобиль».2 В. Поиск всех словоформ, оканчивающихся на заданное пользователем сочетание символов. При запросе «электростанция» обнаруживаются документы, содержащие словоформы «теплоэлектростанция», «гидроэлектростанция»5 Г. Идентифицирует слова, содержащие сочетание символов запроса. Удобно использовать для нахождения документов, содержащих однокоренные слова. При запросе «рабо» идентифицируются такие словоформы, как «работа», «обработка», «работать».4 Д. Обнаруживаются словоформы, начинающиеся с заданной пользователем комбинации символов. При запросе «автомобиль», будет идентифицирована как словоформа «автомобиль», так и иные слова начинающиеся с «автомобиль-», например, «автомобильный».3
13	Расставьте в соответствии программные продукты DLP и их компании-разработчики Компании: 1. SearchInform; 2 Ростелеком; 3. Киберпротект; 4. Стахановец; Программные продукты: A. SearchInform КИБ Б. Кибер Протега В. Стахановец Г. Solar Dozor
14	При внедрении в организации DLP-системы, выполняются следующие мероприятия: 1.Подготовка, 2. Выбор, 3. Установка и настройка, 4. Обучение. Поставьте в соответствие этим мероприятиям, проводимые в это время работы: A. Разработка регламентов для сотрудников; Б. Аудит текущего состояния информационной безопасности в организации; В. Тестирование системы на небольшой группе пользователей или устройствах; Г. Учёт потребностей компании, размера бизнеса, типов данных, которые необходимо защищать, а также возможностей системы для интеграции с другими инструментами безопасности. 1-Б 2-Г 3-В 4-А

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление последовательности

Инструкция: Прочитайте текст и установите правильную последовательность

№ задания	Тексты заданий
15	Установите правильную последовательность перемещения информации в DLP-системе 1. Сборщик информации 2. Источник информации 3. Индексация 4. База данных 5. Анализ 2, 1, 4, 3, 5
16	Пусть есть 4 запроса: A – по атрибутам; F – фразовый; D – по словарю; R – по регулярным. Расставить по порядку от самого быстрого до самого медленного сложные запросы типа: 1. «(A or F or D) and R»; 2. «A and R»; 3. «A or R». 2,1,3
17	Для внедрения DLP-системы в организации проводится ряд мероприятий, перечисленных ниже. Расставьте мероприятия в порядке их выполнения. 1. Установка и настройка 2. Подготовка 3. Выбор

№ задания	Тексты заданий
	4. Обучение 2,3,1,4

БЛОК В (высокий уровень) – Задание открытого типа с развернутым ответом

Инструкция: Прочитайте текст и запишите обоснованный ответ

№ задания	Тексты заданий
18	Специалист по безопасности, организуя автоматизированный поиск информации при расследованиях инцидентов, создает правило (политику безопасности), в котором указывает: - что искать; - где искать; - как часто (расписание); - кого уведомлять в случае нарушения политики.
19	Что позволяет узнать Профайлинг? <i>Профайлинг позволяет узнать многое о личности человека и спрогнозировать его поведение в определенных ситуациях.</i>
20	В работе службы безопасности часто возникают ситуации, когда нужно найти сотрудников, беседующих на определенную тему. Определите примерный список тем, по которым можно сделать вывод о морально-нравственном облике сотрудника. - алкоголь; - наркотики; - долги, кредиты, ипотека и прочие финансовые проблемы; - обсуждение премий и зарплат; - обсуждение руководства; - обсуждение службы ИБ; - терроризм, экстремизм, национализм; - политические взгляды.

**Система оценивания выполнения тестовых заданий по компетенции ПК-3,
формируемой дисциплиной «Аналитика DLP-систем»**

Номер задания	Указания по оцениванию	Результат оценивания (баллы, полученные за выполнение задания/характеристика правильности ответа)
Задания 1-10	Задания с выбором одного или нескольких верных ответов из предложенных считается верным, если правильно указана цифра или цифры, означающие верные ответы.	Совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 11-14	Задания закрытого типа на установление соответствия считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)	Полное совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 15-17	Задания закрытого типа на установление последовательности считается верным, если правильно указана вся последовательность цифр	Полное совпадение с верным ответом оценивается 1 баллом; если допущены ошибки или ответ отсутствует- 0 баллов.
Задания 18-20	Задание открытого типа с развернутым ответом считается верным, если ответ совпадает с эталонным по содержанию и полноте.	Полный правильный ответ на задание оценивается 3 баллами. Если в ответе используются перечисления, то различный порядок следования правильных ответов в перечислении не считается ошибкой; если допущена одна ошибка/неточность/ответ правильный, но не полный - 1 балл, если допущено более одной ошибки/ответ неправильный/ответ отсутствует- 0 баллов.

Ключи к тестовым заданиям по оценке компетенции ПК-3, формируемой дисциплиной «Аналитика DLP-систем»

№ задания	Верный ответ				
1	3				
2	1,2,3,4				
3	1,3,4				
4	1,2,3				
5	1,2,3,4				
6	1,2,3,4				
7	1,2,3,4				
8	3				
9	6				
10	1,3,4,5				
11					
	1	2	3	4	
	В	Г	Б	А	
12					
	1	2	3	4	5
	А	Б	Д	Г	В
13					
	1	2	3	4	
	А	Г	Б	В	
14					
	1	2	3	4	
	Б	Г	В	А	
15	2, 1, 4, 3, 5				
16	2,1,3				
17	2,3,1,4				
18	- что искать; - где искать; - как часто (расписание); - кого уведомлять в случае нарушения политики.				
19	Профайлинг позволяет узнать многое о личности человека и спрогнозировать его поведение в определенных ситуациях.				
20	- алкоголь; - наркотики; - долги, кредиты, ипотека и прочие финансовые проблемы; - обсуждение премий и зарплат; - обсуждение руководства; - обсуждение службы ИБ; - терроризм, экстремизм, национализм; - политические взгляды.				

Методические рекомендации по освоению дисциплины

1. Методические рекомендации преподавателю

Перед началом изучения дисциплины преподаватель должен ознакомить обучающихся с рабочей программой и оценочными материалами по дисциплине, с видами учебной и самостоятельной работы, перечнем литературы и интернет-ресурсов, с формами текущей и промежуточной аттестации, с критериями оценки качества знаний для итоговой оценки по дисциплине.

При проведении лекций, преподаватель:

- 1) формулирует тему и цель занятия, объявляет учебные вопросы;
- 2) излагает основные теоретические положения;
- 3) с помощью технических средств обучения и/или под запись дает определения основных понятий, расчетных формул;
- 4) проводит примеры из отечественного и зарубежного опыта, дает текущие статистические данные для наглядного и образного представления изучаемого материала;
- 5) в конце занятия выдает вопросы для самостоятельного изучения.

На занятиях лабораторного цикла следует обратить внимание на соответствие выбираемых обучающимся средств выполнения решаемым в работе задачам.

Каждая лабораторная работа должна быть оформлена и защищена в соответствии с требованиями. Защита производится после оформления отчета по работе.

Во время выполнения заданий в учебной аудитории обучающийся может консультироваться с преподавателем, определять наиболее эффективные методы решения поставленных задач. Если какая-то часть задания остается не выполненной, обучающийся может продолжить её выполнение во время внеаудиторной самостоятельной работы.

Для оценки полученных знаний и освоения учебного материала по каждому разделу и в целом по дисциплине преподаватель использует формы текущего, промежуточного и итогового контроля знаний обучающихся.

2. Методические рекомендации обучающимся

Приступая к изучению новой учебной дисциплины, обучающиеся должны ознакомиться с рабочей программой, оценочными материалами, учебной, научной и методической литературой, имеющейся в ЭИОС СКФ МТУСИ,

Глубина усвоения дисциплины зависит от активной и систематической работы обучающегося на лекциях и практических занятиях, а также в ходе самостоятельной работы, по изучению рекомендованной литературы.

2.1 Методические указания для обучающихся по лекционным занятиям

Важно сосредоточить внимание на содержании лекции. Это поможет лучше воспринимать учебный материал и уяснить взаимосвязь проблем по всей дисциплине.

Основное содержание лекции целесообразнее записывать в тетради в виде ключевых фраз, понятий, тезисов, обобщений, схем, опорных выводов. Необходимо обращать внимание на термины, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Желательно оставлять в конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющей материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

С целью уяснения теоретических положений, разрешения спорных ситуаций необходимо задавать преподавателю уточняющие вопросы. Для закрепления содержания лекции в памяти, необходимо во время самостоятельной работы внимательно прочесть свой конспект и дополнить его записями из учебников и рекомендованной литературы.

Конспектирование читаемых лекций и их последующая доработка способствует более глубокому усвоению знаний, и поэтому являются важной формой учебной деятельности обучающихся.

2.2 Методические указания для обучающихся по подготовке к лабораторным работам

Лабораторные занятия по любой учебной дисциплине проводятся в соответствии с рабочей программой этой учебной дисциплины в установленные расписанием часы.

Инструктаж по технике безопасности, правилам пожарной безопасности и правилам внутреннего распорядка в лаборатории проводится преподавателем на первом лабораторном занятии. На этом же занятии обучающимся сообщаются:

- программа всего предстоящего лабораторного цикла;
- условия взаимодействия обучающихся с преподавателем в процессе выполнения лабораторных работ;
- условия контроля самостоятельной работы обучающихся, включая правила оформления отчетов по лабораторным работам и их последующей защиты;
- другая необходимая информация.

Организация лабораторных работ включает:

- самостоятельную внеаудиторную подготовку обучающегося к выполнению каждой отдельной лабораторной работы в соответствии с ее программой в рамках часов, выделенных на самостоятельную проработку материала в программе дисциплины;
- входной контроль преподавателем степени подготовленности каждого обучающегося к выполнению лабораторных работ;
- выполнение программы лабораторных работ в полном объеме;
- оформление отчета и его защиту каждым обучающимся в установленные сроки;
- формирование преподавателем рейтингов каждого из обучающихся по результатам выполнения и защиты им отдельных лабораторных работ и их циклов (используется Модульно-рейтинговая система).

Оценка качества выполнения лабораторных работ каждым обучающимся производится преподавателем отдельно за подготовку к работе, ее выполнение и защиту.

Для подготовки и выполнения лабораторных работ используются методические разработки компании СерчИнформ, представленные в электронном виде.

3. Методические рекомендации для обучающихся по самостоятельной работе

Самостоятельная работа обучающихся является составной частью учебной работы и имеет целью закрепление и углубление полученных знаний и навыков, поиск и приобретение новых знаний, в том числе с использованием автоматизированных обучающих курсов (систем), а также выполнение учебных заданий, подготовку к предстоящим занятиям, зачетам и экзаменам.

Самостоятельная работа во внеаудиторное время включает в себя:

- повторение лекционного материала;
- подготовки к лабораторным работам (практическим занятиям);
- изучения учебной и научной литературы;
- решения задач, выданных на практических занятиях;
- подготовки к тестированию;

- выделение наиболее сложных и проблемных вопросов по изучаемой теме, получение разъяснений и рекомендаций по данным вопросам с преподавателями кафедры на их еженедельных консультациях.

- проведение самоконтроля путем ответов на вопросы текущего контроля знаний, решения представленных в учебно-методических материалах кафедры задач, тестов, написания рефератов по отдельным вопросам изучаемой дисциплины.

Самостоятельная работа организуется преподавателями, обеспечивается и контролируется кафедрами. Она предусматривает, как правило, разработку рефератов, выполнение расчетно-графических, вычислительных работ, моделирования и других творческих заданий в соответствии с учебной программой (тематическим планом изучения дисциплины). Основная цель данного вида занятий состоит в обучении курсантов методам самостоятельной работы с учебным материалом.

Материал, подлежащий обработке на самостоятельных занятиях, намечается при разработке программы самостоятельной работы. Опыт, накопленный кафедрами в организации самостоятельных занятий, что материал выделяемый на такие занятия, должен удовлетворять следующим требованиям:

- быть изложенным в учебнике достаточно полно и с примерами;
- обеспечиваться достаточным количеством литературы, учебных пособий, учебно-методических материалов, образцов техники
- содержать материал, углубляющий знания, полученные на лекции;
- осваивать проблемные еще не полностью решенные вопросы.

Перед выполнением внеаудиторной самостоятельной работы преподаватель проводит инструктаж (консультацию) с определением цели задания, его содержания, сроков выполнения, основных требований к результатам работы, критериев оценки, форм контроля и перечня источников и литературы.

Обычно постановку задачи обучаемым на проведение самостоятельной работы преподаватель осуществляет на одном из занятий, предшествующем данному.

Методику самостоятельной работы все обучаемые выбирают индивидуально, но методика достижения конечной цели может определяться преподавателем и включать: последовательность изучения и усвоения учебно-методического материала, пособий, руководств, наставлений, техники и т.д.; определение главного в изучаемом материале, материале, который необходимо законспектировать; просмотр учебных кинофильмов и их обсуждение; работу обучающихся по индивидуальным заданиям; опрос обучаемых в течении 7-10 минут с целью проверки усвоения главного из прочитанного материала.

При возникновении затруднений у обучаемых в разрешении вопросов задания преподавателю необходимо предусмотреть, чтобы каждый обучаемый мог получить оперативную консультацию по любому вопросу, если же при самостоятельной работе возникают затруднения по одному и тому же материалу (вопросу) у многих обучаемых, то желательно провести групповую консультацию.

Для контроля усвоения учебного материала целесообразно проводить в групповое собеседование или обсуждение изучаемого материала, проведение контрольных работ и т.п. Контрольные мероприятия при должной их организации позволяют не только оценивать знания материала, но и углубить и закрепить его у обучаемых.

Приветствуется использование компьютеров, которое:

- расширяет информационную базу учебных занятий;
- повышает активность обучаемых, из пассивного получателя информации они превращаются в её добытчиков;
- способствует развитию способностей к анализу и обобщению, улучшает связанность, широту и глубину мышления;
- облегчает усвоение абстрактного материала, позволяет многое из него представить в виде конкретных образов;
- приучает к точности, аккуратности, последовательности действий способствует

развитию самостоятельности.

Компьютерные технологии и программные продукты для выполнения самостоятельной работы по освоению учебного материала необходимо использовать в соответствии с указаниями методических разработок раздела 5 настоящей Рабочей программы.

Таблица – Учебный материал, выносимый на самостоятельное изучение обучающимся очной формы обучения

№	Темы, разделы, вынесенные на самостоятельную подготовку, вопросы для подготовки к практическим и лабораторным занятиям; курсовые работы, содержание контрольных работ; рекомендации по использованию литературы, ЭВМ и др.	Часов всего: 56	Неделя
Модуль 1 – 28 часов			
1	Защита от несанкционированного доступа к информации. Термины и Определения.	2	1
2	Указ президента российской федерации. Об утверждении перечня сведений конфиденциального характера.	2	2
3	Положение о лицензировании деятельности по технической защите конфиденциальной информации. Постановление Правительства Российской Федерации от 30 апреля 2002 г. № 290.	4	3
4	Доктрина информационной безопасности Российской Федерации;	4	4
5	Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации.	4	5
6	Анализ моделей нарушителя; угрозы информационно-программному обеспечению вычислительных систем и их классификация	4	6
7	Классификация каналов утечки информации.	4	7
8	Требования к современным DLP-системам	4	8
Модуль 2 – 28 часов			
9	Поведенческий анализ. Технология анализа поведения пользователей (User Behavior Analytics, UBA)	2	9
10	Технология цифровых отпечатков (Digital fingerprints, DiFi) сравнивает текстовые, графические и табличные документы с эталонами	2	10
11	Технология графических шаблонов. Технология позволяет контролировать передачу критичных данных в графических форматах	4	11
12	Файловый краулер. Технология позволяет проверять все узлы корпоративной сети и составлять ее наглядную карту, после чего контролировать ресурсы сети.	4	12
13	Технологии глубокого поиска. Поиск изображений, похожих на эталон. Поиск по любым аудио- или видеозаписям действий пользователя. Технология анализа текста. Детектирование текстов, близких по смыслу с эталоном	4	13
14	Технологии пристального наблюдения. Позволяют точно восстанавливать цепочки событий и устанавливать всех причастных к нарушениям	4	14
15	Технология автоматического выявления и группировки неизвестных документов по новым тематикам (кластеризация)	4	15
16	Технология машинного обучения для классификации текста на базе модуля искусственного интеллекта.	4	16

Для более углубленного изучения материала по дисциплине целесообразно использовать учебные курсы сайта <http://www.intuit.ru/>.

Самостоятельная работа обучающихся над усвоением материала по дисциплине может выполняться в помещении для самостоятельной работы СКФ МТУСИ, посредством использования электронной библиотеки и ЭИОС.