**Образовательная автономная некоммерческая организация**
**высшего профессионального образования**

**«МОСКОВСКИЙ ОТКРЫТЫЙ ИНСТИТУТ»**

# Темы курсовых работ по дисциплине «Информационная безопасность»

1 Современная законодательно-нормативная база защиты государственной тайны
2 Роль информационного права и информационной безопасности в современном обществе
3 Назначение и структура системы защиты информации коммерческого предприятия
4 Особенности работы с персоналом, владеющим конфиденциальной информацией
5 Методика инструктирования и обучения персонала правилами защиты секретов фирмы
6 Система защиты информации в зарубежных странах
7 Система защиты информации в банковских системах
8 Система защиты информации в системах страхования
9 Методика защиты информации в системах электронного документооборота
10 Виды и состав угроз информационной безопасности
11 Классификация и характеристика видов, методов и средств защиты информации и их соотношение с объектами защиты
12 Защита информации в процессе переговоров и совещаний
13 Методики отбора персонала для работы с конфиденциальной информацией
14 Защита сетевой инфраструктуры предприятия
15 Система защиты коммерческой тайны малого коммерческого предприятия
16 Организационные вопросы использования DLP систем на средних коммерческих предприятиях
17 Технические и организационные подходы к защите VoIP систем предприятия
18 Методические подходы к разработке правил ИБ для файрволлов
19 Методические подходы к разработке правил ИБ для файлового сервера
20 Разработка комплекса мер по антивирусной защите ИС на примере сети малого предприятия
21 Методические подходы к разработке правил расследования инцидентов в области ИБ

22 Защита информации в распределенных образовательных системах
23 Построение модели угроз малого предприятия розничной торговли продуктами питания
24 Построение модели угроз малого предприятия сервисного центра компьютерной техники
25 Методические подходы к разработке правил анализа безопасности использования прикладного ПО
26 Обзор методов и средств анализа сетевого трафика и поиска аномалий трафика
27 Использование DLP-систем для осуществления контроля каналов коммуникаций предприятия
28 Обеспечение защиты корпоративных информационных ресурсов от утечек информации при помощи DLP-систем
29 Управление инцидентами информационной безопасности с использованием возможностей DLP-систем
30 Программные комплексы анализа каналов утечки информации
31 Разработка концепции и структуры построения системы управления инцидентами информационной безопасности в организации
32 Методики обхода систем предотвращения утечек данных (DLP)
33 Методика расследования преднамеренных действий, связанных с нецелевым использованием информационных ресурсов организации
34 Контроль ограничения доступа к конфиденциальной информации сотрудников ИТ-подразделений средствами DLP-систем
35 Практические аспекты использования различных видов поиска в DLP-системах
36 Сравнительный анализ подходов к вопросам управления инцидентами информационной безопасности в российской и международной практике
37 Системы предотвращения утечек конфиденциальной информации (DLP)
38 Принципы построения и функционирования DLP-систем
39 Разработка классификации инцидентов информационной безопасности
40 Сравнительный анализ различных подходов к оценке ущерба, возникающего вследствие инцидента информационной безопасности
41 Особенности применения основных способов и методов выявления различных инцидентов информационной безопасности
42 Современные технические средства выявления инцидентов информационной безопасности
43 Проблемы автоматизации процессов управления инцидентами информационной безопасности

44 Разработка системы менеджмента рисков информационной безопасности в составе общих бизнес-рисков организации
45 Разработка методики выявления инцидентов информационной безопасности, связанных с нарушением политики использования электронной почтовой системы организации
46 Разработка методики выявления инцидентов информационной безопасности, связанных с нарушением политики использования информационных ресурсов организации
47 Разработка методики выявления инцидентов информационной безопасности, связанных с нарушением политики использования информационных систем организации
48 Разработка методики расследования инцидентов информационной безопасности, связанных с преднамеренной утечкой информации
49 Разработка методики расследования инцидентов информационной безопасности, связанных со случайной утечкой информации
50 Разработка методики расследования действий, связанных с несанкционированным подключением к локальной сети посторонних устройств
51 Разработка методики расследования действий, связанных с использованием АРМ и информационных ресурсов организации в не служебных целях
52 Разработка методики расследования действий, связанных с компрометацией парольной информации для доступа к локальной сети и информационным системам организации
53 Разработка методики расследования преднамеренных действий, связанных с нарушением порядка доступа к информационным ресурсам и системам (попытка несанкционированного доступа)
54 Разработка методики расследования преднамеренных действий, связанных с несанкционированным копированием конфиденциальной информации на съемный носитель
55 Разработка методики расследования преднамеренных действий, связанных с несанкционированной распечаткой конфиденциальной информации
56 Разработка методики расследования преднамеренных действий, связанных с размещением конфиденциальной информации на общих информационных ресурсах организации
57 Разработка методики проведения мониторинга действий пользователей с целью соблюдения политики информационной безопасности

58 Разработка модели (схемы) взаимодействий между подразделением информационной безопасности и подразделением информационных технологий, а также другими подразделениями организации при расследовании инцидентов информационной безопасности
59 Разработка рекомендаций по сбору и оценке событий информационной безопасности
60 Разработка рекомендаций по документированию событий информационной безопасности и обновления базы данных событий/инцидентов информационной безопасности
61 Современная законодательно-нормативная база защиты государственной тайны
62 Роль информационного права и информационной безопасности в современном обществе
63 Назначение и структура системы защиты информации коммерческого предприятия
64 Особенности работы с персоналом, владеющим конфиденциальной информацией
65 Методика инструктирования и обучения персонала правилами защиты секретов фирмы
66 Система защиты информации в зарубежных странах
67 Система защиты информации в банковских системах
68 Система защиты информации в системах страхования
69 Методика защиты информации в системах электронного документооборота
70 Виды и состав угроз информационной безопасности
71 Классификация и характеристика видов, методов и средств защиты информации и их соотношение с объектами защиты
72 Защита информации в процессе переговоров и совещаний
73 Методики отбора персонала для работы с конфиденциальной информацией
74 Защита сетевой инфраструктуры предприятия
75 Система защиты коммерческой тайны малого коммерческого предприятия
76 Организационные вопросы использования DLP систем на средних коммерческих предприятиях
77 Технические и организационные подходы к защите VoIP систем предприятия
78 Методические подходы к разработке правил ИБ для файрволлов
79 Методические подходы к разработке правил ИБ для файлового сервера

80 Разработка комплекса мер по антивирусной защите ИС на примере сети малого предприятия
81 Методические подходы к разработке правил расследования инцидентов в области ИБ
82 Защита информации в распределенных образовательных системах
83 Построение модели угроз малого предприятия розничной торговли продуктами питания
84 Построение модели угроз малого предприятия сервисного центра компьютерной техники
85 Методические подходы к разработке правил анализа безопасности использования прикладного ПО
86 Обзор методов и средств анализа сетевого трафика и поиска аномалий трафика
87 Использование DLP-систем для осуществления контроля каналов коммуникаций предприятия
88 Обеспечение защиты корпоративных информационных ресурсов от утечек информации при помощи DLP-систем
89 Управление инцидентами информационной безопасности с использованием возможностей DLP-систем
90 Программные комплексы анализа каналов утечки информации
91 Разработка концепции и структуры построения системы управления инцидентами информационной безопасности в организации
92 Методики обхода систем предотвращения утечек данных (DLP)
93 Методика расследования преднамеренных действий, связанных с нецелевым использованием информационных ресурсов организации
94 Контроль ограничения доступа к конфиденциальной информации сотрудников ИТ-подразделений средствами DLP-систем
95 Практические аспекты использования различных видов поиска в DLP-системах
96 Сравнительный анализ подходов к вопросам управления инцидентами информационной безопасности в российской и международной практике
97 Системы предотвращения утечек конфиденциальной информации (DLP)
98 Принципы построения и функционирования DLP-систем
99 Разработка классификации инцидентов информационной безопасности
100 Сравнительный анализ различных подходов к оценке ущерба, возникающего вследствие инцидента информационной безопасности
101 Особенности применения основных способов и методов выявления различных инцидентов информационной безопасности

102 Современные технические средства выявления инцидентов информационной безопасности
103 Проблемы автоматизации процессов управления инцидентами информационной безопасности
104 Разработка системы менеджмента рисков информационной безопасности в составе общих бизнес-рисков организации
105 Разработка методики выявления инцидентов информационной безопасности, связанных с нарушением политики использования электронной почтовой системы организации
106 Разработка методики выявления инцидентов информационной безопасности, связанных с нарушением политики использования информационных ресурсов организации
107 Разработка методики выявления инцидентов информационной безопасности, связанных с нарушением политики использования информационных систем организации
108 Разработка методики расследования инцидентов информационной безопасности, связанных с преднамеренной утечкой информации
109 Разработка методики расследования инцидентов информационной безопасности, связанных со случайной утечкой информации
110 Разработка методики расследования действий, связанных с несанкционированным подключением к локальной сети посторонних устройств
111 Разработка методики расследования действий, связанных с использованием АРМ и информационных ресурсов организации в не служебных целях
112 Разработка методики расследования действий, связанных с компрометацией парольной информации для доступа к локальной сети и информационным системам организации
113 Разработка методики расследования преднамеренных действий, связанных с нарушением порядка доступа к информационным ресурсам и системам (попытка несанкционированного доступа)
114 Разработка методики расследования преднамеренных действий, связанных с несанкционированным копированием конфиденциальной информации на съемный носитель
115 Разработка методики расследования преднамеренных действий, связанных с несанкционированной распечаткой конфиденциальной информации
116 Разработка методики расследования преднамеренных действий, связанных с размещением конфиденциальной информации на общих информационных ресурсах организации

117 Разработка методики проведения мониторинга действий пользователей с целью соблюдения политики информационной безопасности
118 Разработка модели (схемы) взаимодействий между подразделением информационной безопасности и подразделением информационных технологий, а также другими подразделениями организации при расследовании инцидентов информационной безопасности
119 Разработка рекомендаций по сбору и оценке событий информационной безопасности
120 Разработка рекомендаций по документированию событий информационной безопасности и обновления базы данных событий/инцидентов информационной безопасности