

УТВЕРЖДАЮ
 Декан факультета

 (подпись) Шматко А. Д.
 «___» _____ 20__
 ФИО

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА

Направление/специальность подготовки	38.03.05 Бизнес-информатика
Специализация/профиль/программа подготовки	Управление технологиями искусственного интеллекта
Уровень высшего образования	Бакалавриат
Форма обучения	Очная
Факультет	Р Международного промышленного менеджмента и коммуникации
Выпускающая кафедра	Р1 МЕНЕДЖМЕНТ ОРГАНИЗАЦИИ
Кафедра-разработчик рабочей программы	Р1 МЕНЕДЖМЕНТ ОРГАНИЗАЦИИ

КУРС	СЕМЕСТР	ОБЩАЯ ТРУДОЁМКОСТЬ (ЗАЧЕТНЫХ ЕДИНИЦ)	ЧАСЫ (по наличию видов занятий)									ВИД ПРОМЕЖУТОЧНОГО КОНТРОЛЯ
			ОБЩАЯ ТРУДОЁМКОСТЬ	АУДИТОРНЫЕ ЗАНЯТИЯ				САМОСТОЯТЕЛЬНАЯ РАБОТА				
				ВСЕГО	ЛЕКЦИИ	ЛАБОРАТОРНЫЙ ПРАКТИКУМ	ПРАКТИЧЕСКИЕ ЗАНЯТИЯ	ВСЕГО	КУРСОВОЙ ПРОЕКТ	КУРСОВАЯ РАБОТА	ДРУГИЕ ВИДЫ САМОСТ. РАБОТЫ	
3	5	4	144	51	17	0	34	93	0	0	93	ЭКЗ.

ЛИСТ СОГЛАСОВАНИЯ

РАБОЧАЯ ПРОГРАММА СОСТАВЛЕНА В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ ФЕДЕРАЛЬНОГО
ГОСУДАРСТВЕННОГО ОБРАЗОВАТЕЛЬНОГО СТАНДАРТА ВЫСШЕГО ОБРАЗОВАНИЯ (ФГОС ВО)

38.03.05 Бизнес-информатика

год набора группы: 2024

Программу составил:

Кафедра Р1 МЕНЕДЖМЕНТ ОРГАНИЗАЦИИ
Волкова Анастасия Анатольевна, к.э.н., доцент

Программа рассмотрена
на заседании кафедры-разработчика
рабочей программы **Р1 МЕНЕДЖМЕНТ ОРГАНИЗАЦИИ**

Заведующий кафедрой Шматко А.Д., д.э.н., проф.

Программа рассмотрена
на заседании выпускающей кафедры

Р1 МЕНЕДЖМЕНТ ОРГАНИЗАЦИИ

Заведующий кафедрой Шматко А.Д., д.э.н., проф.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА

Разделы рабочей программы

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО
3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ
4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ
5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ
6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Приложения к рабочей программе дисциплины

- Приложение 1. Аннотация рабочей программы
- Приложение 2. Технологии и формы обучения
- Приложение 3. Фонды оценочных средств

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является формирование следующих компетенций:

ПСК-6 — способность управлять информационной безопасностью ресурсов информационных технологий

Формированию компетенций служит достижение следующих результатов образования:

ПСК-6

знания:

знать технологии и программные средства защиты информации;

умения:

уметь адекватно реагировать на различные угрозы информационной безопасности, применять современные технологии защиты информации;

навыки:

владеть навыком реализации алгоритмических и программных способов защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина **ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА** является дисциплиной **части, формируемой участниками образовательных отношений блока 1**, программы подготовки по направлению *38.03.05 Бизнес-информатика*.

Содержание дисциплины является логическим продолжением дисциплин: **МАТЕМАТИКА 1: ДИФФЕРЕНЦИАЛЬНОЕ ИСЧИСЛЕНИЕ, ВВЕДЕНИЕ В ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ПРОГРАММИРОВАНИЕ**.

Содержание дисциплины является основой для освоения дисциплин: **ИНФОРМАЦИОННЫЕ СИСТЕМЫ В ЛОГИСТИКЕ, ИНФОРМАЦИОННЫЕ СИСТЕМЫ В УПРАВЛЕНИИ МАРКЕТИНГОМ, ИНФОРМАЦИОННЫЕ СИСТЕМЫ В УПРАВЛЕНИИ ПРОДАЖАМИ, УПРАВЛЕНИЕ ИНФОРМАЦИОННО-ТЕХНИЧЕСКИМИ ПРОЕКТАМИ, ИНТЕРНЕТ-ТЕХНОЛОГИИ В БИЗНЕСЕ**.

Предварительные компетенции, сформированные у обучающегося до начала изучения дисциплины:

- ОПК-3 — способен управлять процессами создания и использования продуктов и услуг в сфере информационно-коммуникационных технологий, в том числе разрабатывать алгоритмы и программы для их практической реализации
- ОПК-4 — Способен понимать принципы работы информационных технологий; использовать информацию, методы и программные средства ее сбора, обработки и анализа для информационно-аналитической поддержки принятия управленческих решений
- ПК-91 — способен к коммуникации и кооперации в цифровой среде, использованию различных цифровых средств, позволяющих во взаимодействии с другими людьми достигать поставленных целей
- ПК-94 — способен к управлению информацией и данными, поиску источников информации и данных, восприятию, анализу, запоминанию и передаче информации с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными с целью эффективного использования полученной информации для решения задач
- ПК-95 — способен к критическому мышлению в цифровой среде, оценке информации, ее достоверности, построению логических умозаключений на основании поступающих информации и данных
- УК-1 — Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 4 з.е., 144 ч.

3.1. Содержание (дидактика) дисциплины

КУРС	СЕМЕСТР	Наименование разделов и дидактических единиц	ВСЕГО	Аудиторные занятия в контактной форме			Самостоятельная работа студентов	Формируемая компетенция, %
				ВСЕГО	Лекции	Практические занятия		ПСК-6
3	5	Раздел 1. Раздел 1. Основные составляющие информационной безопасности. Основные понятия информационной безопасности. Классификация угроз. Классификация средств защиты информации. Методы и средства организационно-правовой защиты информации. Методы и средства инженерно-технической защиты. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности.	29	10	4	6	19	20
3	5	Раздел 2. Раздел 2. Правовое обеспечение информационной безопасности. Информация, информационные технологии и защита информации. Безопасность персональных данных. Результаты интеллектуальной деятельности. Авторское право. Право промышленной собственности. Коммерческая тайна и правовой режим обеспечения ее безопасности. Государственная тайна и ее правовая защита. Электронная подпись и правовое обеспечение безопасности переписки. Правовое обеспечение безопасности при использовании сетей связи. Характеристика и последствия преступлений в сфере информационной безопасности.	28	10	4	6	18	20
3	5	Раздел 3. Раздел 3. Организационное обеспечение информационной безопасности. Государственная система обеспечения информационной безопасности. Организация работ по защите конфиденциальной информации. Лицензирование.	32	12	4	8	20	20
3	5	Раздел 4. Раздел 4. Защита информации в современных информационных системах. Способы контактного и бесконтактного съема информации. Возможности атаки на ОС, их классификация. Парольная защита ПК. Взлом паролей Windows NT и UNIX. Защита от взлома. Идентификация и аутентификация пользователей ОС. Windows, UNIX, Linux. Формальные модели защищаемых систем и их применение в современных ОС. Методы и средства ограничения доступа к ресурсам и компонентам ПК.	26	10	2	8	16	20
3	5	Раздел 5. Раздел 5. Защита информации в компьютерных сетях. Основные угрозы безопасности сетей. Модели угроз и модели противодействия. Методы аутентификации пользователей в сети. Разновидности вирусных программ. Программные средства защиты: сканеры вирусов, сетевая защита, брандмауэры и др. Системы обнаружения сетевого вторжения. Безопасность глобальных сетей и электронной почты.	29	9	3	6	20	20
Всего за 5 семестр			144	51	17	34	93	100
Всего по дисциплине			144	51	17	34	93	100

3.2. Аудиторный практикум

№ п/п	Номер и наименование раздела дисциплины	Тема практического занятия	Объем, ауд. часов
1	Раздел 1. Раздел 1. Основные составляющие информационной безопасности.	Основные составляющие информационной безопасности.	6
2	Раздел 2. Раздел 2. Правовое обеспечение информационной безопасности.	Правовое обеспечение информационной безопасности.	6
3	Раздел 3. Раздел 3. Организационное обеспечение информационной безопасности.	Организационное обеспечение информационной безопасности.	8
4	Раздел 4. Раздел 4. Защита информации в современных информационных системах.	Защита информации в современных информационных системах.	8
5	Раздел 5. Раздел 5. Защита информации в компьютерных сетях.	Основные составляющие информационной безопасности.	6
Всего за 5 семестр			34

3.3. Самостоятельная работа студента (СРС)

№ п/п	Номер и наименование раздела дисциплины	Содержание учебного задания	Объем, часов
1	Раздел 1. Раздел 1. Основные составляющие информационной безопасности.	Основные составляющие информационной безопасности.	19
2	Раздел 2. Раздел 2. Правовое обеспечение информационной безопасности.	Правовое обеспечение информационной безопасности.	18
3	Раздел 3. Раздел 3. Организационное обеспечение информационной безопасности.	Организационное обеспечение информационной безопасности.	20

4	Раздел 4. Раздел 4. Защита информации в современных информационных системах.	Защита информации в современных информационных системах.	16
5	Раздел 5. Раздел 5. Защита информации в компьютерных сетях.	Основные составляющие информационной безопасности.	20
Всего за 5 семестр			93

4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

СЕМЕСТР	НЕДЕЛИ СЕМЕСТРА																
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
5	Отч. по ПЗ	Отч. по ПЗ	Отч. по ПЗ	Отч. по ПЗ	Отч. по ПЗ	ДР	Отч. по ПЗ	Отч. по ПЗ	Отч. по ПЗ	ДР	Отч. по ПЗ	Отч. по ПЗ	Отч. по ПЗ	Отч. по ПЗ	Отч. по ПЗ	ДР	Отч. по ПЗ

Условные обозначения:

- ДР – диагностическая работа;
- Отч. по ПЗ – отчет по практическому заданию.

Текущий контроль успеваемости студентов проводится в дискретные временные интервалы в следующих формах:

- диагностическая работа;
- отчет по практическому заданию.

Промежуточная аттестация проводится в формах:

- экзамен.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература по дисциплине:

1. А. А. Стрельцов, В. Н. Пожарский, В. А. Минаев. . Организационно-правовое обеспечение информационной безопасности. М.: Изд-во МГТУ им. Н. Э. Баумана, 2018, эл. рес.
2. Организационное и правовое обеспечение информационной безопасности. Москва: Юрайт, 2019, эл. рес.
3. С. А. Нестеров. . Информационная безопасность. Москва: Юрайт, 2019, эл. рес.

5.2. Дополнительная литература по дисциплине:

не требуется.

5.3. Периодические издания:

1. Информационно-измерительные и управляющие системы;
2. Моделирование и анализ информационных систем;
3. Прикладная информатика.

5.4. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины, электронные библиотечные системы:

не требуется.

Современные профессиональные базы данных:

1. <https://rusneb.ru> – Национальная электронная библиотека (НЭБ);
2. <https://cyberleninka.ru/> - Научная электронная библиотека «Киберленинка»;
<http://www.rfbr.ru/rffi/ru/library> - Полнотекстовая электронная библиотека Российского фонда фундаментальных исследований.

Информационные справочные системы:

1. Техэксперт – Информационный портал технического регулирования: Нормы, правила, стандарты РФ;
2. http://library.voenmeh.ru/jirbis2/index.php?option=com_irbis&view=irbis&Itemid=457 - БД ГОСТов собственной генерации БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова;
3. <http://www.consultant.ru/>- КонсультантПлюс- информационный портал правовой информации.

5.5. Программное обеспечение:

не требуется.

5.6. Информационные технологии:

взаимодействие с обучающимися посредством ЭИОС Moodle БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Лекционные занятия:

специализированные требования по оборудованию отсутствуют; аудитория с посадочными местами по количеству студентов; доска.

6.2. Практические занятия:

1. Проектор;
2. Рабочее лабораторное место.

6.3. Прочее:

1. рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
2. рабочие места студентов, оснащенные компьютерами с доступом в Интернет, предназначенные для работы в электронной образовательной среде.

Аннотация рабочей программы

Дисциплина **ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА** является дисциплиной **части, формируемой участниками образовательных отношений блока 1**, программы подготовки по направлению *38.03.05 Бизнес-информатика*. Дисциплина реализуется на факультете *Р* Международного промышленного менеджмента и коммуникации БГТУ "ВОЕНМЕХ" им. Д.Ф. Устинова кафедрой **Р1 МЕНЕДЖМЕНТ ОРГАНИЗАЦИИ**.

Дисциплина нацелена на формирование *компетенций*:
ПСК-6 способность управлять информационной безопасностью ресурсов информационных технологий.

Содержание дисциплины охватывает круг вопросов, связанных с основными понятиями и составляющими информационной безопасности, видами угроз и комплексом мер по их нейтрализации.

Программой дисциплины предусмотрены следующие **виды контроля**:

Текущий контроль успеваемости студентов проводится в дискретные временные интервалы в следующих формах:

- диагностическая работа;
- отчет по практическому заданию.

Промежуточная аттестация проводится в формах:

- экзамен.

Общая трудоемкость освоения дисциплины составляет **4 з.е., 144 ч.** Программой дисциплины предусмотрены лекционные занятия (**17 ч.**), практические занятия (**34 ч.**), самостоятельная работа студента (**93 ч.**).

ТЕХНОЛОГИИ И ФОРМЫ ОБУЧЕНИЯ

Рекомендации по освоению дисциплины для студента

Трудоемкость освоения дисциплины составляет 144 ч., из них 51 ч. аудиторных занятий, и 93 ч., отведенных на самостоятельную работу студента.

Рекомендации по распределению учебного времени по видам самостоятельной работы и разделам дисциплины приведены в таблице.

Контроль освоения дисциплины производится в соответствии с Положением о текущем, рубежном контроле успеваемости и промежуточной аттестации обучающихся.

Формы контроля и критерии оценивания приведены в приложении 3 к Рабочей программе.

Наименование работы	Рекомендуемая литература	Трудоемкость, час.
Раздел 1. Раздел 1. Основные составляющие информационной безопасности.		
Основные составляющие информационной безопасности.	С. А. Нестеров. . Информационная безопасность: Москва: Юрайт, 2019 (1-4)	19
Итого по разделу 1		19
Раздел 2. Раздел 2. Правовое обеспечение информационной безопасности.		
Правовое обеспечение информационной безопасности.	А. А. Стрельцов, В. Н. Пожарский, В. А. Минаев. . Организационно-правовое обеспечение информационной безопасности: М.: Изд-во МГТУ им. Н. Э. Баумана, 2018 (1-4)	18
Итого по разделу 2		18
Раздел 3. Раздел 3. Организационное обеспечение информационной безопасности.		
Организационное обеспечение информационной безопасности.	Организационное и правовое обеспечение информационной безопасности: Москва: Юрайт, 2019 (1-3)	20
Итого по разделу 3		20
Раздел 4. Раздел 4. Защита информации в современных информационных системах.		
Защита информации в современных информационных системах.	С. А. Нестеров. . Информационная безопасность: Москва: Юрайт, 2019 (1-2)	16
Итого по разделу 4		16
Раздел 5. Раздел 5. Защита информации в компьютерных сетях.		
Основные составляющие информационной безопасности.	А. А. Стрельцов, В. Н. Пожарский, В. А. Минаев. . Организационно-правовое обеспечение информационной безопасности: М.: Изд-во МГТУ им. Н. Э. Баумана, 2018 (1-2)	20
Итого по разделу 5		20

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств, позволяющие оценить результаты обучения по данной дисциплине, включают в себя:

- диагностическая работа
- отчет по практическому заданию;
- экзамен.

Критерии оценивания

Диагностическая работа

Диагностическая работа проводится в форме теста в ЭИОС Moodle:

- при правильном ответе менее чем на 60% вопросов - не аттестация;
- при правильном ответе на 60% вопросов и более - аттестация.

Отчет по практическому заданию

Требования к выполнению практических заданий (ПЗ):

По всем ПЗ необходимо выполнить поставленную задачу согласно заданию, а также внимательно прочитать сопутствующую информацию о программном обеспечении, в котором осуществляется работа.

Отчет по ПЗ:

По каждому ПЗ необходимо подготовить отчет в электронном виде. После выполнения отчета его необходимо предоставить на проверку преподавателю (либо лично, либо посредством электронной почты). При оформлении отчета руководствоваться ГОСТ 7.32-2017. Состав отчета описывается в постановке задачи каждого ПЗ.

Защита ПЗ:

Защита ПЗ предусматривает обсуждение порядка решения предусмотренных его тематикой задач, включая проверку усвоения студентом соответствующих сведений из теории.

Типовые практические задания включены в состав УМК дисциплины.

Экзамен

Обучающийся имеет право на получение минимальной положительной оценки при условии успешного прохождения текущего контроля успеваемости в форме диагностической работы в соответствии с графиком раздела 4.

Итоговый контроль по дисциплине проходит в форме экзамена. Допуск к экзамену оформляется при условии полного выполнения всех мероприятий, предусмотренных графиком контрольных мероприятий. Экзаменационный билет включает в себя два теоретических вопроса. Комплект вопросов к экзамену размещен в УМК дисциплины.

Паспорт фонда оценочных средств

КУРС	СЕМЕСТР	Наименование разделов и дидактических единиц	ВСЕГО	Аудиторные занятия в контактной форме			Самостоятельная работа студентов	Формируемая компетенция, %	НАИМЕНОВАНИЕ ОЦЕНОЧНОГО СРЕДСТВА
				ВСЕГО	Лекции	Практические занятия		ПСК-6	
3	5	Раздел 1. Раздел 1. Основные составляющие информационной безопасности.	29	10	4	6	19	20	Отчет по практическому заданию
3	5	Раздел 2. Раздел 2. Правовое обеспечение информационной безопасности.	28	10	4	6	18	20	Отчет по практическому заданию
3	5	Раздел 3. Раздел 3. Организационное обеспечение информационной безопасности.	32	12	4	8	20	20	Отчет по практическому заданию
3	5	Раздел 4. Раздел 4. Защита информации в современных информационных системах.	26	10	2	8	16	20	Отчет по практическому заданию
3	5	Раздел 5. Раздел 5. Защита информации в компьютерных сетях.	29	9	3	6	20	20	Отчет по практическому заданию
Всего за 5 семестр			144	51	17	34	93	100	
Всего по дисциплине			144	51	17	34	93	100	

Критерии оценивания

ПСК-6

Вопросы открытого типа:

- № 1 Что такое принцип наименьших привилегий и как его реализация способствует повышению уровня информационной безопасности?
- № 2 Какую роль играет шифрование данных в обеспечении информационной безопасности?
- № 3 Что такое управление рисками в информационной безопасности и какие этапы включает этот процесс?
- № 4 Какие преимущества и недостатки имеет двухфакторная аутентификация (2FA)?
- № 5 Как функционирует система обнаружения вторжений (IDS) и как она может помочь в предотвращении угроз?
- № 6 Что такое политика информационной безопасности и какие основные элементы она должна включать?
- № 7 Какие ключевые аспекты нужно учитывать при разработке плана восстановления после инцидентов информационной безопасности?
- № 8 Что представляет собой концепция Zero Trust и как она изменяет подход к информационной безопасности?
- № 9 Какие меры можно предпринять для защиты данных, хранящихся в облачных средах?
- № 10 Что такое управление инцидентами информационной безопасности и какие шаги включает этот процесс?

Вопросы закрытого типа:

- № 1 Что представляет собой риск в контексте информационной безопасности?
- А. Возможность нарушения конфиденциальности
 - Б. Вероятность возникновения угрозы
 - В. Последствия атаки
 - Г. Уязвимость системы
- № 2 Какая из следующих мер направлена на предотвращение угроз?
- А. Шифрование данных
 - Б. Восстановление после сбоя
 - В. Резервное копирование данных
 - Г. Аудит безопасности
- № 3 Какой из следующих подходов наиболее подходит для управления рисками информационной безопасности?
- А. Подход, основанный на анализе вероятностей и последствий угроз
 - Б. Подход, основанный на интуиции и экспертном мнении
 - В. Подход, основанный на исторических данных
 - Г. Подход, ориентированный на минимизацию затрат
- № 4 1. Какая из перечисленных технологий лучше всего подходит для защиты данных, находящихся в облачной среде?
- А. Виртуальная частная сеть (VPN)
 - Б. Физическое ограничение доступа к серверам
 - В. Шифрование данных в состоянии покоя и при передаче
 - Г. Инструменты для обнаружения вторжений (IDS)
- № 5 1. Какой метод мониторинга наиболее эффективен для обнаружения аномалий в сетевом трафике, указывающих на возможные угрозы?
- А. Ручное отслеживание логов
 - Б. Использование системы анализа сетевого трафика на основе машинного обучения
 - В. Периодическая проверка журналов безопасности
 - Г. Установка антивирусного ПО на конечные устройства

- № 6
1. Какой из следующих методов наиболее эффективно защищает систему от несанкционированного доступа?
- А. Использование многофакторной аутентификации
 - Б. Регулярное изменение паролей
 - В. Ограничение прав доступа
 - Г. Установка антивирусного ПО
- № 7
1. Какой из следующих подходов используется для минимизации ущерба в случае компрометации учетной записи?
- А. Внедрение однофакторной аутентификации
 - Б. Ограничение доступа по времени и месту
 - В. Политика обязательного изменения пароля раз в 90 дней
 - Г. Ведение журнала всех операций
- № 8
1. Что является основным назначением DLP (Data Loss Prevention) систем?
- А. Шифрование данных
 - Б. Обнаружение вторжений
 - В. Предотвращение утечки конфиденциальной информации
 - Г. Управление доступом к сети
- № 9
1. Какую функцию выполняют системы управления событиями и информацией безопасности (SIEM)?
- А. Сбор, анализ и корреляция данных о событиях безопасности для обнаружения угроз
 - Б. Шифрование данных в реальном времени
 - В. Мониторинг сетевого трафика
 - Г. Управление привилегиями пользователей
- № 10
1. Какую роль играет аудит безопасности в процессе управления информационной безопасностью?
- А. Реализация политик безопасности
 - Б. Оценка эффективности существующих мер безопасности и выявление уязвимостей
 - В. Фильтрация контента
 - Г. Управление доступом к сети