

Минобрнауки России

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»  
(ФГБОУ ВО «ВГУ»)

**УТВЕРЖДАЮ**

Заведующий кафедрой  
Борисов Дмитрий Николаевич  
Кафедра информационных систем

03.05.2023

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ**

Б1.В.05 Безопасность информационных систем

**1. Код и наименование направления подготовки/специальности:**

09.03.02 Информационные системы и технологии

**2. Профиль подготовки/специализация:** Информационные системы и сетевые технологии

**3. Квалификация (степень) выпускника:**

Бакалавриат

**4. Форма обучения:**

Очная

**5. Кафедра, отвечающая за реализацию дисциплины:**

Кафедра информационных систем

**6. Составители программы:**

Ермаков Михаил Викторович

**7. Рекомендована:** НМС ФКН, протокол №7 от 03.05.2023

**8. Учебный год:**

2026-2027

**9. Цели и задачи учебной дисциплины:**

*Цель освоения учебной дисциплины: приобретение знаний и навыков в области технологии и практики работы информационных систем с точки зрения безопасности, формирование системного подхода к проектированию аспектов безопасности и формирование критического подхода к используемым информационным системам и технологиям.*

*Задачи учебной дисциплины: в результате освоения дисциплины студент должен: знать:*

- стандарты описания архитектуры информационных систем;
- стандарты безопасности ИС;
- нормативно-правовую базу обеспечения безопасности в РФ;

- основные пути дискредитации ИС;
- основные методы защиты ИС;
- современные программные и аппаратные средства защиты;
- технологии разработки объектов безопасности в областях приборостроения, техники, связи, ТП, телекоммуникации;
- методы и средства сборки и интеграции программных модулей и компонент, методы и средства верификации работоспособности программных продуктов;
- устройство и функционирование современных ИС, протоколы, интерфейсы и форматы обмена данными;
- современные средства, позволяющие создавать цифровые двойники, deepfake в различных областях и возможности анализа большого объёма разнородной информации;
- угрозы, связанные с активным внедрением робототехники, роботики и интернета вещей;
- современные, перспективные и устаревшие протоколы связи, а также угрозы, связанные с их прямым или косвенным использованием;
- возможности, предоставляемые технологией blockchain.

уметь:

- строить модели безопасности и нарушителя для ИС;
- дать правовую оценку мер обеспечения безопасности;
- обеспечивать соблюдение требований при разработке и тестировании ИС;
- собирать программные компоненты в программный продукт;
- подключать программные компоненты к компонентам внешней среды;
- проверять работоспособность программных продуктов;
- использовать современные приложения и сервисы для анализа и восстановления систем;
- фиксировать состояние среды для последующего анализа;
- разрабатывать код компонентов ИС и баз данных ИС.

владеть:

- навыками оценки угроз безопасности;
- средствами антивирусной защиты, VPN, FireWall, наблюдения за трафиком и т.п.;
- современными средствами разработки и интеграции ПО, средствами коммуникации.

#### **10. Место учебной дисциплины в структуре ООП:**

Дисциплина относится к обязательным дисциплинам вариативной части профессионального цикла.

Для изучения дисциплины необходимо ориентироваться в современных информационных технологиях, сетевых средствах, физике (механика, оптика, электричество).

В результате изучения студенты должны ориентироваться в современных стандартах и технологиях, связанных с безопасностью, уметь выделить уязвимые места различных реальных информационных систем и предложить методы их локализации и устранения.

#### **11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников) и индикаторами их достижения:**

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
<p>ПК-2 Способен выполнять интеграцию программных модулей и компонент, выполнять верификацию программных продуктов</p>	<p>ПК-2.1 Знает методы и средства сборки и интеграции программных модулей и компонент, методы и средства верификации работоспособности программных продуктов  ПК-2.2 Собирает программные компоненты в программный продукт  ПК-2.3 Подключает программные компоненты к компонентам внешней среды  ПК-2.4 Проверяет работоспособность программных продуктов</p>	<p>знать:</p> <ul style="list-style-type: none"> <li>- стандарты описания архитектуры информационных систем;</li> </ul> <p>уметь:</p> <ul style="list-style-type: none"> <li>- разрабатывать алгоритмы;</li> <li>- применять стандарты;</li> <li>- давать оценку надёжности используемых и разработанных алгоритмов и моделей.</li> </ul> <ul style="list-style-type: none"> <li>- собирать программные компоненты в программный продукт;</li> <li>- подключать программные компоненты к компонентам внешней среды;</li> <li>- проверять работоспособность программных продуктов;</li> </ul> <p>владеть:</p> <ul style="list-style-type: none"> <li>- навыками оценки угроз;</li> <li>- методы и средства сборки и интеграции программных модулей и компонент, методы и средства верификации работоспособности программных продуктов;</li> <li>- современными средствами разработки и интеграции ПО, средствами коммуникации.</li> </ul>
<p>ПК-3 Способен выполнять работы по созданию (модификации) и сопровождению информационных систем</p>	<p>ПК-3.2 Знает устройство и функционирование современных ИС, протоколы, интерфейсы и форматы обмена данными  ПК-3.4 Разрабатывает код компонентов ИС и баз данных ИС  ПК-3.5 Настраивает и устанавливает операционную систему, СУБД, прикладное ПО, необходимое для функционирования ИС</p>	<p>знать:</p> <ul style="list-style-type: none"> <li>- стандарты описания архитектуры информационных систем; - стандарты безопасности ИС;</li> <li>- нормативно-правовую базу обеспечения безопасности в РФ;</li> </ul> <ul style="list-style-type: none"> <li>- устройство и функционирование современных ИС, протоколы, интерфейсы и форматы обмена данными;</li> <li>- современные средства, позволяющие создавать цифровые двойники, deepfake в различных областях и возможности анализа большого объёма разнородной информации;</li> <li>- угрозы, связанные с активным внедрением робототехники, роботики и интернета вещей;</li> <li>- современные, перспективные и устаревшие протоколы связи, а также угрозы, связанные с их прямым или косвенным использованием;</li> <li>- возможности, предоставляемые технологией blockchain</li> </ul> <p>уметь:</p>

		<ul style="list-style-type: none"> <li>- строить модели безопасности и нарушителя для ИС;</li> <li>- обеспечивать соблюдение требований при разработке и тестировании ИС;</li> <li>- использовать современные приложения и сервисы для анализа и восстановления систем;</li> <li>- фиксировать состояние среды для последующего анализа;</li> <li>- разрабатывать код компонентов ИС и баз данных ИС.</li> <li>-</li> </ul> <p>владеть:</p> <ul style="list-style-type: none"> <li>- навыками оценки угроз безопасности;</li> <li>- средствами антивирусной защиты, VPN, FireWall, наблюдения за трафиком и т.п.</li> </ul>
--	--	---

**12. Объем дисциплины в зачетных единицах/час:**

2/72

**Форма промежуточной аттестации:**

Зачет

**13. Трудоемкость по видам учебной работы**

Вид учебной работы	Семестр 7	Всего
Аудиторные занятия	32	32
Лекционные занятия	16	16
Практические занятия	-	-
Лабораторные занятия	16	16
Самостоятельная работа	40	40
Курсовая работа	-	-
Промежуточная аттестация	-	-
Часы на контроль	-	-
Всего	72	72

**13.1. Содержание дисциплины**

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1	<p>Безопасность информационных систем. Обзор курса.</p> <p>Существующие, возникающие и прогнозируемые угрозы нарушения безопасности информационных систем.</p> <p>Влияние развития современных технологий (BigData, ИИ, виртуальная реальность, робототехника, интернет вещей, блокчейн, высокоскоростные беспроводные сети) на изменение векторов угроз.</p>	<p>Знакомство. Основные понятия курса и связь их с уже изученными ранее (и изучаемыми параллельно) предметами.</p> <p>Ознакомление со структурой курса.</p> <p>Определение приоритетов.</p> <p>Использование информационных систем в различных областях деятельности человека.</p> <p>Критически важные области использования информационных систем. Существующие угрозы, их опасность и методы ее снижения.</p> <p>Угрозы, связанные с развитием современных технологий.</p> <p>Прогнозирование угроз будущего.</p> <p>Локализация и ликвидация последствий нарушения безопасности.</p>	id=12083
2	<p>Законодательная и нормативно-правовая база РФ в области безопасности информационных систем</p>	<p>Законодательство СССР. Стратегия национальной безопасности РФ. Законы и подзаконные акты РФ в области защиты информации и безопасности. Уголовное законодательство. Соответствие отечественного законодательства в области безопасности зарубежному.</p> <p>Перспективы законодательства: регулирование использования blockchain, сетей связи, роботизации, применения ИИ и т.п.</p>	id=12083
3	<p>Системы отечественной сертификации информационных систем по вопросам безопасности. Иностранные стандарты в области защиты информационных систем</p>	<p>Система сертификации в РФ, Государственная техническая комиссия.</p> <p>Министерство обороны. Федеральная служба безопасности. Прочие системы сертификации.</p> <p>Система стандартов США. Стандарты стран Евросоюза. Взаимодействие межнациональных государственных и коммерческих информационных систем.</p>	id=12083

4	Анализ требований стандартов применительно к современным информационным системам	Основные понятия. Анализ требований ГТК к СВТ. Анализ требований ГТК к АС. Анализ требований на отсутствие не декларированных возможностей. Критика отечественных стандартов в области защиты информации.	id=12083
5	Роль криптографии и криптоанализа в обеспечении безопасности систем.	Использование криптографии в целях обеспечения безопасности систем. Криптография с открытым ключом: основы криптостойкости. Криптография с закрытым ключом: эволюция алгоритмов. Криптоанализ и его роль в обеспечении безопасности ИС, Квантовая криптография. Роль криптографии в обеспечении безопасности высокоскоростных сетей связи.	id=12083
6	Проводные и беспроводные линии связи	Определение и распределение акцентов безопасности. Сети общего доступа и специализированные сети. Физическая организация сетей. Проводные и беспроводные методы связи. Надёжность и безопасность их использования. Интернет как основа общедоступной сети. Особенности регулирования операторов связи. Применение и надёжность криптографических средств.	id=12083
7	Виртуальные частные сети	Основные понятия. Использование сетей общего пользования для организации корпоративных информационных систем. Принципы построения VPN. Программные и аппаратные средства реализации VPN. Необходимость использования VPN в современных системах управления и связи. Требования к сетям.	id=12083
8	Системы обнаружения атак. Защита от внутренних атак.	Основные понятия. Цели использования систем. Проблемы сбора данных и методы их анализа. Ответные действия системы. Обзор существующих систем. Классификация внутренних атак. Работа с персоналом для предотвращения возникновения атак. Защита от атак Low and slow. Перспективы защиты от атак в системах, управляемых ИИ. Социальная инженерия.	id=12083

9	<p>Антивирусная защита. Централизованное управление системой безопасности</p>	<p>Вирусы. Причины появления. Последствия вирусных атак. Классификация вирусов. Классификация антивирусов. Централизованное управление антивирусной защитой. Спам и защита электронной почты. Структура системы безопасности информационных систем. Проблемы взаимодействия отдельных подсистем. Функционирование распределенных информационных систем. Централизованное и децентрализованное управление системой.</p>	id=12083
10	<p>Проблема электронного документооборота и электронных архивов</p>	<p>Проблемы обработки документов в электронной форме. Законодательство в области электронных документов и архивов. Системы электронного документооборота. Большие данные и защита их использования. Право на управление доступом к собственным персональным данным. Использование blockchain для обеспечения целостности данных и проблема уничтожения данных.</p>	id=12083
11	<p>Защита операционных систем Классификация операционных систем по уровню безопасности</p>	<p>Средства безопасности операционных систем Microsoft. Средства безопасности операционных систем типа UNIX. Защищенные операционные системы (зарубежные и отечественные). Интеграция системы безопасности информационной системы с ОС. Несовпадение понятий безопасности различных ИС между собой и ОС. Защита встроенных операционных систем и ПО контроллеров. Особенности функционирования «умных» устройств.</p>	id=12083
12	<p>Защита баз данных и средств доступа к ним</p>	<p>Использование СУБД в информационных системах. Классификация СУБД. Особенности СУБД с точки зрения обеспечения безопасности. Расширенная защита с СУБД. Интеграция систем безопасности СУБД, ОС и ИС между собой. Особенности защиты больших баз данных. Угрозы для баз данных со стороны высокоскоростных линий связи.</p>	id=12083

13	Компьютерная криминалистика	Причины появления и применения. Фиксация доказательств. Точки применения. Средства анализа. Результаты. Отличия криминалистики от защиты. Работа с deepfake. Использование ИИ и Bigdata для решения задач.	id=12083
14	Биометрические системы идентификации и аутентификации	Физические основы биометрии, перспективные и широко используемые системы и датчики, ошибки систем биометрического распознавания, обман таких систем. Юридические особенности использования биометрического подтверждения личности и последствия компрометации биометрических систем.	id=12083
15	Виртуализация вычислительных систем и сетей	Безопасность использования виртуализированной среды. Атаки на виртуальные машины и сети. Виртуализация систем безопасности. Система-в-системе. Атаки на хост-системы и их последствия. Системы безопасности облачных сред.	id=12083
16	Нейроинтерфейсы, роботизация и безопасность использования роботизированных систем	Уязвимости существующего имплантируемого и сопрягаемого с человеком оборудования. Угрозы со стороны беспилотных систем и ИИ. Защита систем от деструктивных внешних воздействий, в частности систем РЭБ. Безопасность систем в случае отказа высокоинтеллектуальных систем.	id=12083

### 13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
1	Безопасность информационных систем. Угрозы нарушения безопасности	1		1	2	4



2	Законодательная и нормативно-правовая база РФ	1		1	3	5
3	Системы отечественной сертификации и иностранные стандарты	1		1	2	4
4	Анализ требований стандартов	1		1	2	4
5	Роль криптографии и криптоанализа	1		1	2	4
6	Проводные и беспроводные линии связи	1		1	3	5
7	Виртуальные частные сети	1		1	2	4
8	Системы обнаружения атак и защита от внутренних атак	1		1	2	4
9	Антивирусная защита. Централизованное управление системой безопасности	1		1	3	5
10	Проблема электронного документооборота	1		1	2	4
11	Защита операционных систем	1		1	3	5
12	Защита баз данных и средств доступа к ним	1		1	3	5

13	Компьютерная криминалистика	1		1	3	5
14	Биометрические системы	1		1	3	5
15	Виртуализация	1		1	3	5
16	Нейроинтерфейсы и роботизация	1		1	2	4
		16	0	16	40	72

#### 14. Методические указания для обучающихся по освоению дисциплины

Приступая к изучению дисциплины, студенту необходимо внимательно ознакомиться с тематическим планом занятий, списком рекомендованной литературы. Следует уяснить последовательность выполнения индивидуальных учебных заданий.

Самостоятельная работа студента предполагает работу с научной и учебной литературой, современной информационной средой, умение извлекать факты.

Уровень и глубина усвоения дисциплины зависят от активной и систематической работы на Лекциях и самостоятельно работы по поиску и обработке новых фактов и тенденций.

При изучении дисциплины студенты выполняют следующие задания:

- изучают рекомендованную научно-практическую и учебную литературу;
- изучают информационную среду, связанную с тематикой лекций;
- выполняют задания, предусмотренные для самостоятельной работы.

Основными видами аудиторной работы студентов являются лекции и лабораторные занятия.

В ходе лекций преподаватель излагает и разъясняет основные, наиболее сложные понятия темы, а также связанные с ней теоретические и практические проблемы, дает рекомендации на лабораторное занятие и указания на самостоятельную работу.

Лабораторные занятия завершают изучение наиболее важных тем учебной дисциплины. Они служат для закрепления изученного материала, развития умений и навыков подготовки докладов, сообщений, приобретения опыта устных публичных выступлений, ведения дискуссии, аргументации и защиты выдвигаемых положений, а также для контроля преподавателем степени подготовленности студентов по изучаемой дисциплине.

Лабораторные занятия предполагают свободный обмен мнениями по избранной тематике. Он начинается со вступительного слова преподавателя, формулирующего цель занятия и характеризующего его основную проблематику. Затем, как правило, заслушиваются сообщения студентов. Обсуждение сообщения совмещается с рассмотрением намеченных вопросов. Сообщения, предполагающие анализ публикаций по отдельным вопросам семинара, заслушиваются обычно в середине занятия. Поощряется выдвижение и обсуждение альтернативных мнений. В заключительном слове преподаватель подводит итоги обсуждения. В целях контроля подготовленности студентов и привития им навыков краткого письменного изложения своих мыслей преподаватель в ходе занятий может осуществлять текущий контроль знаний в виде тестовых заданий.

При подготовке студенты имеют возможность воспользоваться консультациями преподавателя. Кроме указанных тем студенты вправе, по согласованию с преподавателем, избирать и другие интересующие их темы.

При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей, вовремя подключаться к online занятиям, ответственно подходить к заданиям для самостоятельной работы.

**15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины**

№ п/п	Источник
1	Бирюков, А. А. Информационная безопасность: защита и нападение / Бирюков А.А. — Москва : ДМК Пресс, 2012. — 474 с. <URL: <a href="http://e.lanbook.com/books/element.php?pl1_id=39990">http://e.lanbook.com/books/element.php?pl1_id=39990</a> >
2	Шаньгин, В. Ф. Информационная безопасность / Шаньгин В.Ф. — Москва : ДМК Пресс, 2014 . — 702 с. <URL: <a href="http://e.lanbook.com/books/element.php?pl1_id=50578">http://e.lanbook.com/books/element.php?pl1_id=50578</a> >
3	Ищейнов, В.Я. Информационная безопасность и защита информации : учебное пособие : [16+] / В.Я. Ищейнов .— Москва; Берлин : Директ-Медиа, 2020 .— 271 с. — ISBN 978-5-4499-0496-6 .— <URL: <a href="http://biblioclub.ru/index.php?page=book&amp;id=571485">http://biblioclub.ru/index.php?page=book&amp;id=571485</a> >.
4	Ерохин, В.В. Безопасность информационных систем : учебное пособие / В.В. Ерохин, Д.А. Погонишева, И.Г. Степченко .— 3-е изд., стер. — Москва : Флинта, 2016 .— 184 с. — ISBN 978-5-9765-1904-6 .— <URL: <a href="http://biblioclub.ru/index.php?page=book_red&amp;id=562458">http://biblioclub.ru/index.php?page=book_red&amp;id=562458</a> >.
5	Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов / В.И. Аверченков [и др.] .— 4-е изд., стер. — Москва : Флинта, 2016 .— 224 с. — (Организация и технология защиты информации) .— ISBN 978-5-9765-1274-0 .— <URL: <a href="http://biblioclub.ru/index.php?page=book&amp;id=93351">http://biblioclub.ru/index.php?page=book&amp;id=93351</a> >.

**б) дополнительная литература:**

№ п/п	Источник
1	<a href="#">Паласиос, Х.</a> . Unity 5.x. Программирование искусственного интеллекта в играх [Электронный ресурс] / Паласиос Х. ; Пер. с англ. Рагимова Р.Н. — Москва : ДМК Пресс, 2017 .— 272 с. — Книга из коллекции ДМК Пресс - Информатика .— ISBN 978-5-97060-436-6 .— <URL: <a href="https://e.lanbook.com/book/97348">https://e.lanbook.com/book/97348</a> >.
2	Осипов, Г.С. Методы искусственного интеллекта / Г.С. Осипов .— Москва : Физматлит, 2011 .— 296 с. — ISBN 978-5-9221-1323-6 .— <URL: <a href="https://biblioclub.ru/index.php?page=book_red&amp;id=457464">https://biblioclub.ru/index.php?page=book_red&amp;id=457464</a> >.
3	Джонс, М. Т. Программирование искусственного интеллекта в приложениях [Электронный ресурс] / Джонс М. Т. — Москва : ДМК Пресс, 2011 .— 312 с. — Книга из коллекции ДМК Пресс - Информатика .— ISBN 978-5-94074-746-8 .— <URL: <a href="http://e.lanbook.com/books/element.php?pl1_cid=25&amp;pl1_id=1244">http://e.lanbook.com/books/element.php?pl1_cid=25&amp;pl1_id=1244</a> >.

**в) информационные электронно-образовательные ресурсы:**

№ п/п	Источник
-------	----------

1	Образовательный портал ВГУ edu.vsu.ru
2	Научная электронная библиотека <a href="https://elibrary.ru/">https://elibrary.ru/</a>
3	Электронная библиотека учебно-методических материалов ВГУ <a href="http://www.lib.vsu.ru/cgi-bin/zgate?Init+lib.xml,simple.xml+rus">http://www.lib.vsu.ru/cgi-bin/zgate?Init+lib.xml,simple.xml+rus</a>
4	Российская национальная библиотека <a href="http://nlr.ru/">http://nlr.ru/</a>
5	<a href="http://www.lib.vsu.ru">www.lib.vsu.ru</a> ЗНБ ВГУ

#### 16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Необходима самостоятельная подготовка по темам, которые рассматриваются на лекциях.
2	Для подготовки к лабораторному занятию необходимо выполнить расширенный поиск по тематике занятия. Лабораторное занятие предполагает наличие у студента свежайшей информации на рассматриваемую тему – сообщения по угрозам, уязвимостям, конференциям, изменениям законодательства и т.п.

#### 17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение):

1. Презентационные материалы в различных форматах.
2. Вычислительная сеть для обмена информацией и демонстрации презентаций.
3. Различное ПО, упоминаемое на занятиях в случае, если необходимо продемонстрировать его функциональность или уязвимость.
4. Технологии электронного обучения и дистанционные образовательные технологии на базе портала edu.vsu.ru, а также другие доступные ресурсы сети интернет.

#### 18. Материально-техническое обеспечение дисциплины:

1. Лекционная аудитория, оборудованная мультимедийным проектором.
2. Компьютерные классы факультета для проведения лабораторных занятий.
3. Портал «Электронный университет ВГУ» <http://lms.vsu.ru> для организации и методического обеспечения самостоятельной работы студентов.

#### 19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
1	<p>Безопасность информационных систем</p> <p>Угрозы нарушения безопасности</p> <p>Законодательная и нормативно-правовая база РФ Системы отечественной сертификации</p> <p>Иностранные стандарты</p> <p>Анализ требований стандартов</p> <p>Централизованное управление системой безопасности Проблема электронного документооборота</p> <p>Компьютерная криминалистика</p> <p>Биометрические системы</p> <p>Виртуализация Нейроинтерфейсы и роботизация</p>	ПК 2	ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4	Опрос, реферат по одной из тем.
2	<p>Анализ требований стандартов Роль криптографии и криптоанализа</p> <p>Проводные и беспроводные линии связи</p> <p>Виртуальные частные сети</p> <p>Системы обнаружения атак</p> <p>Защита от внутренних атак</p> <p>Антивирусная защита</p> <p>Централизованное управление системой безопасности Проблема электронного документооборота</p> <p>Защита операционных систем</p> <p>Защита баз данных и средств доступа к ним Виртуализация</p>	ПК-3	ПК-3.2 ПК-3.4 ПК-3.5	Опрос, реферат по одной из тем.

Промежуточная аттестация

Форма контроля - Зачет

Оценочные средства для промежуточной аттестации Темы рефератов:

1. Понятие безопасности в современных условиях.
2. Законодательная и нормативно-правовая база защиты информации в РФ.
3. Понятия «модель угроз» и «модель нарушителя».
4. Система сертификации ФСТЭК. (СЗИ НСД СВТ, СЗИ НСД АС. Критерии и т.п.)
5. Классификация систем защиты в Европе и США
6. Межсетевые экраны. Обзор достоинств и недостатков существующих коммерческих и некоммерческих межсетевых экранов
7. Виртуальные частные сети. Обзор достоинств и недостатков существующих средств создания VPN
8. Сетевые системы обнаружения атак. Host-системы обнаружения атак. Обзор достоинств и недостатков существующих средств обнаружения атак.
9. Системы защиты от внутренних атак
10. Вирусы и Антивирусная защита. Обзор существующих антивирусных средств.
11. Биометрия. Принципы, параметры.
12. Криптозащита и криптоанализ
13. Защита почтовых программ, web-трафика и защита от spama.
14. Физическая защита информационных систем от утечки информации
15. Защита настольных и серверных операционных систем.
16. Защита СУБД.
17. Мобильные операционные системы и их защита.
18. Беспроводные технологии и их защита.
19. Облачные системы хранения и обработки. Их защита.
20. Компьютерная криминалистика.
21. Защита интернета вещей.
22. Использование blockchain в системах обмена информацией.
23. Нейроинтерфейсы и сопрягаемое с человеком оборудование.
24. Перспективы и угрозы ИИ

## **20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания**

### **20.1 Текущий контроль успеваемости**

Контроль успеваемости по дисциплине осуществляется с помощью устного опроса в рамках практических занятий.

Оценивание студентов по результатам промежуточных аттестаций осуществляется в соответствии с Положением о балльно-рейтинговой системе факультета компьютерных наук.

Для оценивания результатов обучения на зачете используются следующие показатели:

1. Знание теоретического учебного материала и владение понятийным аппаратом

– 25 баллов за каждую из 3-х текущих аттестаций.

2. Умение применять полученные знания при построении практических моделей – 25 баллов за каждую из 3-х текущих аттестаций.
3. Владение навыками построения моделей, обеспечивающей безопасность и целостность данных в информационных системах – 50 баллов.

Итоговая оценка по 100-балльной шкале складывается:

- из 25 баллов, получаемых путем усреднения оценок, полученных за теоретическую часть курса по трем текущим аттестациям;

- из 25 баллов, получаемых путем усреднения оценок, полученных за работу на лабораторных занятиях;
- из 50 баллов, получаемых за подготовку отчётного реферата и его защиту.

Итоговая оценка за зачет по пятибалльной шкале выводится в соответствии с Положением о балльно-рейтинговой системе факультета компьютерных наук по следующим правилам:

Зачтено – от 50 до 69 баллов,

Не зачтено – менее 50 баллов.

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся в полной мере владеет понятийным аппаратом данной области науки (теоретическими основами дисциплины), способен иллюстрировать ответ примерами, фактами, применять теоретические знания для решения практических задач в области безопасности информационных систем.	<i>Повышенный уровень</i>	<i>Зачтено</i>
Обучающийся допускает ошибки или пропуски при подготовке ответов. Допускает ошибки при защите собственных ответов на зачёте, но даёт правильные ответы на дополнительные вопросы.	<i>Базовый уровень</i>	<i>Зачтено</i>
Обучающийся допускает грубые ошибки при подготовке ответов. Может не учитывать современные направления в области изучаемой дисциплины, допускает ошибки при защите заданий на зачёте, и не может дать правильные ответы на дополнительные вопросы.	<i>Пороговый уровень</i>	<i>Зачтено</i>
Обучающийся не может сформулировать грамотного, даже устаревшего ответа на поставленные задачи, допускает грубые ошибки при защите заданий на зачёте, и не даёт правильные ответы на дополнительные вопросы.	–	<i>Не зачтено</i>

Приведённые ниже задания рекомендуется использовать при проведении диагностических работ для оценки остаточных знаний по дисциплине.

### **Компетенция ПК-2:**

К правовым методам, обеспечивающим информационную безопасность, относятся:

- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий

С) Разработка и конкретизация правовых нормативных актов обеспечения безопасности  
ANSWER: С

Основными источниками угроз информационной безопасности являются все указанное в списке:

- А) Хищение жестких дисков, подключение к сети, инсайдерство
  - В) Перехват данных, хищение данных, изменение архитектуры системы
  - С) Хищение данных, подкуп системных администраторов, нарушение регламента работы
- ANSWER: В

Виды информационной безопасности:

- А) Персональная, корпоративная, государственная
- В) Клиентская, серверная, сетевая
- С) Локальная, глобальная, смешанная

ANSWER: А

Цели информационной безопасности – своевременное обнаружение, предупреждение:

- А) несанкционированного доступа, воздействия в сети
- В) инсайдерства в организации
- С) чрезвычайных ситуаций

ANSWER: А

Основные объекты информационной безопасности:

- А) Компьютерные сети, базы данных
- В) Информационные системы, психологическое состояние пользователей
- С) Бизнес-ориентированные, коммерческие системы

ANSWER: А

Основными рисками информационной безопасности являются:

- А) Искажение, уменьшение объема, перекодировка информации
- В) Техническое вмешательство, выведение из строя оборудования сети
- С) Потеря, искажение, утечка информации

ANSWER: С

К основным принципам обеспечения информационной безопасности относится:

- А) Экономической эффективности системы безопасности
- В) Многоплатформенной реализации системы
- С) Усиления защищенности всех звеньев системы

ANSWER: А

Основными субъектами информационной безопасности являются:

- А) руководители, менеджеры, администраторы компаний
- В) органы права, государства, бизнеса
- С) сетевые базы данных, фаерволлы

ANSWER: В

К основным функциям системы безопасности можно отнести все перечисленное:

- А) Установление регламента, аудит системы, выявление рисков
- В) Установка новых офисных приложений, смена хостинг-компания
- С) Внедрение аутентификации, проверки контактных данных пользователей

ANSWER: А

Принципом информационной безопасности является принцип недопущения:

- А) Неоправданных ограничений при работе в сети (системе)
- В) Рисков безопасности сети, системы
- С) Презумпции секретности

ANSWER: А

Принципом политики информационной безопасности является принцип:

- А) Невозможности миновать защитные средства сети (системы)
- В) Усиления основного звена сети, системы
- С) Полного блокирования доступа при риск-ситуациях

ANSWER: А

Принципом политики информационной безопасности является принцип:



- A) Усиления защищенности самого незащищенного звена сети (системы)
- B) Перехода в безопасное состояние работы сети, системы
- C) Полного доступа пользователей ко всем ресурсам сети, системы

ANSWER: A

Принципом политики информационной безопасности является принцип:

- A) Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- B) Одноуровневой защиты сети, системы
- C) Совместимых, однотипных программно-технических средств сети, системы

ANSWER: A

К основным типам средств воздействия на компьютерную сеть относится:

- A) Компьютерный сбой
- B) Логические закладки («мины»)
- C) Аварийное отключение питания

ANSWER: B

Когда получен спам по e-mail с приложенным файлом, следует:

- A) Прочитать приложение, если оно не содержит ничего ценного – удалить
- B) Сохранить приложение в папке «Спам», выяснить затем IP-адрес генератора спама
- C) Удалить письмо с приложением, не раскрывая (не читая) его

ANSWER: C

Принцип Кирхгофа:

- A) Секретность ключа определена секретностью открытого сообщения
- B) Секретность информации определена скоростью передачи данных
- C) Секретность закрытого сообщения определяется секретностью ключа

ANSWER: C

ЭЦП – это:

- A) Электронно-цифровой преобразователь
- B) Электронно-цифровая подпись
- C) Электронно-цифровой процессор

ANSWER: B

Наиболее распространены угрозы информационной безопасности корпоративной системы:

- A) Покупка нелегального ПО
- B) Ошибки эксплуатации и неумышленного изменения режима работы системы
- C) Сознательного внедрения сетевых вирусов

ANSWER: B

Наиболее распространены угрозы информационной безопасности сети:

- A) Распределенный доступ клиент, отказ оборудования
- B) Моральный износ сети, инсайдерство
- C) Сбой (отказ) оборудования, нелегальное копирование данных

ANSWER: C

Наиболее распространены средства воздействия на сеть офиса:

- A) Слабый трафик, информационный обман, вирусы в интернет
- B) Вирусы в сети, логические мины (закладки), информационный перехват
- C) Компьютерные сбои, изменение администрирования, топологии

ANSWER: B

Утечкой информации в системе называется ситуация, характеризуемая:

- A) Потерей данных в системе
- B) Изменением формы информации
- C) Изменением содержания информации

ANSWER: A

Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

- A) Целостность
- B) Доступность
- C) Актуальность

ANSWER: A

Угроза информационной системе (компьютерной сети) – это:

- A) Вероятное событие
- B) Детерминированное (всегда определенное) событие
- C) Событие, происходящее периодически

ANSWER: A

Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

- A) Регламентированной
- B) Правовой
- C) Защищаемой

ANSWER: C

Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке:

- A) Программные, технические, организационные, технологические
- B) Серверные, клиентские, спутниковые, наземные
- C) Личные, корпоративные, социальные, национальные

ANSWER: A

Окончательно, ответственность за защищенность данных в компьютерной сети несет:

- A) Владелец сети
- B) Администратор сети
- C) Пользователь сети

ANSWER: A

Политика безопасности в системе (сети) – это комплекс:

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

ANSWER: A

Наиболее важным при реализации защитных мер политики безопасности является:

- A) Аудит, анализ затрат на проведение защитных мер
- B) Аудит, анализ безопасности
- C) Аудит, анализ уязвимостей, риск-ситуаций

ANSWER: C

### **Компетенция ПК-3:**

## Объекты

Основные объекты информационной безопасности:			МС
Балл по умолчанию:			1
Случайный порядок ответов			Да
Нумеровать варианты ответов?			0
Штраф за каждую неправильную попытку:			100
ID-номер:			
#	Ответы	Отзыв	Оценка
A.	Компьютерные сети, базы данных		100
B.	Информационные системы, психологическое состояние пользователей		-100
C.	Бизнес-ориентированные, коммерческие системы		-100
<b>Общий отзыв к вопросу:</b>			
<b>Для любого правильного ответа:</b>		Ваш ответ верный.	
<b>Для любого неправильного ответа:</b>		Ваш ответ неправильный.	
<b>Подсказка 1:</b>			
<b>Показать количество правильных ответов (Подсказка 1):</b>		Нет	
<b>Удалить некорректные ответы (Подсказка 1):</b>		Нет	
<b>Теги:</b>			
Позволяет выбрать один или несколько правильных ответов из заданного списка. (МС/МА)			

## Ответственность

Ответственность за защищенность данных в компьютерной сети несет			MC
Балл по умолчанию:			1
Случайный порядок ответов			Да
Нумеровать варианты ответов?			0
Штраф за каждую неправильную попытку:			100
ID-номер:			
#	Ответы	Отзыв	Оценка
A.	Владелец сети		100
B.	Администратор сети		-100
C.	Пользователь сети		-100
D.	Хакер		-100
Общий отзыв к вопросу:			
Для любого правильного ответа:		Ваш ответ верный.	
Для любого неправильного ответа:		Ваш ответ неправильный.	
Подсказка 1:			
Показать количество правильных ответов (Подсказка 1):		Нет	
Удалить некорректные ответы (Подсказка 1):		Нет	
Теги:			
Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)			

## Угроза ИС

Угроза информационной системе – это			МС
Балл по умолчанию:			1
Случайный порядок ответов			Да
Нумеровать варианты ответов?			0
Штраф за каждую неправильную попытку:			100
ID-номер:			
#	Ответы	Отзыв	Оценка
A.	Вероятное событие		100
B.	Детерминированное (всегда определенное) событие		-100
C.	Событие, происходящее периодически		-100
<b>Общий отзыв к вопросу:</b>			
<b>Для любого правильного ответа:</b>		Ваш ответ верный.	
<b>Для любого неправильного ответа:</b>		Ваш ответ неправильный.	
<b>Подсказка 1:</b>			
<b>Показать количество правильных ответов (Подсказка 1):</b>		Нет	
<b>Удалить некорректные ответы (Подсказка 1):</b>		Нет	
<b>Теги:</b>			
Позволяет выбирать один или несколько правильных ответов из заданного списка. (МС/МА)			

## Угрозы ИБ

Наиболее распространены угрозы информационной безопасности корпоративной системы			MC
Балл по умолчанию:			1
Случайный порядок ответов			Да
Нумеровать варианты ответов?			0
Штраф за каждую неправильную попытку:			100
ID-номер:			
#	Ответы	Отзыв	Оценка
A.	Использование нелегального ПО		-100
B.	Ошибки эксплуатации и неумышленного изменения режима работы системы		100
C.	Сознательного внедрения сетевых вирусов		-100
<b>Общий отзыв к вопросу:</b>			
<b>Для любого правильного ответа:</b>		Ваш ответ верный.	
<b>Для любого неправильного ответа:</b>		Ваш ответ неправильный.	
<b>Подсказка 1:</b>			
<b>Показать количество правильных ответов (Подсказка 1):</b>		Нет	
<b>Удалить некорректные ответы (Подсказка 1):</b>		Нет	
<b>Теги:</b>			
Позволяет выбрать один или несколько правильных ответов из заданного списка. (MC/MA)			

## ЭЦП

Что такое ЭЦП			МА
Балл по умолчанию:			1
Случайный порядок ответов			Да
Нумеровать варианты ответов?			0
Показать количество правильных ответов после окончания:			Да
Штраф за каждую неправильную попытку:			100
ID-номер:			
#	Ответы	Отзыв	Оценка
А.	Электронно-цифровой преобразователь		-50
В.	Электронно-цифровая подпись		100
С.	Электронно-цифровой процессор		-50
<b>Общий отзыв к вопросу:</b>			
<b>Для любого правильного ответа:</b>		Ваш ответ верный.	
<b>Для любого неправильного ответа:</b>		Ваш ответ неправильный.	
<b>Для любого частично правильного ответа:</b>		Ваш ответ частично правильный.	
<b>Подсказка 1:</b>			
<b>Показать количество правильных ответов (Подсказка 1):</b>		Нет	
<b>Удалить некорректные ответы (Подсказка 1):</b>		Нет	
<b>Теги:</b>			
<i>Позволяет выбирать один или несколько правильных ответов из заданного списка. (МС/МА)</i>			

## Длительность восстановления сети.

Команда системных администраторов компании составляет 5 человек. 20 % персонала компании болеет, в отпуске или в командировке.			NUM
Сеть компании насчитывает 400 компьютеров.			
Сколько времени потребуется на восстановление сети после сбоя, в результате которого были выведены из строя 25% компьютеров компании.			
Типичное время сканирования одного компьютера - 1 час,			
Типичное время восстановления повреждённого компьютера - 5 часов.			
ТК не нарушаем; считаем, что и сканирование и восстановление требует полного внимания оператора.			
<b>Балл по умолчанию:</b>			2
<b>Штраф за каждую неправильную попытку:</b>			33.3
<b>ID-номер:</b>			
#	Ответы	Отзыв	Оценка
A.	28.125		100
	<b>Общий отзыв к вопросу:</b>	В рабочих днях	
	<b>Подсказка 1:</b>		
	<b>Показать количество правильных ответов (Подсказка 1):</b>	Нет	
	<b>Удалить некорректные ответы (Подсказка 1):</b>	Нет	
	<b>Теги:</b>		
<i>Импортирование этого типа вопроса не поддерживается.</i>			

## Мощность DDOS-атаки

Рассчитайте мощность DDOS-атаки если в ней используется бот-нет из 50000 устройств посылающих по 1000 запросов с секунду с размером пакета 128 байт.			NUM	
<b>Балл по умолчанию:</b>				1
<b>Штраф за каждую неправильную попытку:</b>				100
<b>ID-номер:</b>				
#	Ответы	Отзыв		Оценка
A.	6.25		100	
	<b>Общий отзыв к вопросу:</b>	В Гбитах в секунду		
	<b>Подсказка 1:</b>			
	<b>Показать количество правильных ответов (Подсказка 1):</b>	Нет		
	<b>Удалить некорректные ответы (Подсказка 1):</b>	Нет		
	<b>Теги:</b>			
<i>Импортирование этого типа вопроса не поддерживается.</i>				



## Открытые точки доступа WI-FI

Опишите риск использования открытых точек доступа Wi-Fi.		ES
<b>Балл по умолчанию:</b>		3
<b>Формат ответа:</b>		HTML-редактор
<b>Требовать текст:</b>		Да
<b>Размер поля:</b>		15
<b>Разрешить вложения:</b>		0
<b>Требуемое число вложений:</b>		0
<b>Разрешенные типы файлов:</b>		
<b>ID-номер:</b>		
	<b>Шаблон ответа</b>	<b>Информация для оценивающих</b>
		<p>В отличном ответе (3 балла) должна быть указана основная проблема - возможность организации злоумышленником фиктивных точек доступа, которые будут выдавать себя за открытую сеть, но при установке соединения смогут собирать весь трафик и все процедуры установки защищённых соединений внутри Wi-fi соединения.</p> <p>В случае, если в ответе будут приведены рассуждения о безопасности Wi-fi, протоколах, их версиях и эти рассуждения будут правильными, то оценка 2</p> <p>В случае, если в ответе будет просто указано, что в этом случае трафик будет не защищён, оценка 1</p>
	<b>Общий отзыв к вопросу:</b>	
	<b>Теги:</b>	
<i>Допускает в ответе загрузить файл и/или ввести текст. Ответ должен быть оценен преподавателем вручную.</i>		

## Функции современных антивирусных решений

Опишите пожалуйста функции современных антивирусных решений. Приведите примеры.		ES
<b>Балл по умолчанию:</b>		3
<b>Формат ответа:</b>		HTML-редактор
<b>Требовать текст:</b>		Да
<b>Размер поля:</b>		15
<b>Разрешить вложения:</b>		0
<b>Требуемое число вложений:</b>		0
<b>Разрешенные типы файлов:</b>		
<b>ID-номер:</b>		
	<b>Шаблон ответа</b>	<b>Информация для оценивающих</b>
		<p>В ответе должны быть отражены</p> <ul style="list-style-type: none"> <li>- кроссплатформенность решения</li> <li>- разнонаправленность решения (контроль файлов, приложений, сетевой активности ... )</li> <li>- менеджер паролей</li> <li>- родительский контроль</li> <li>- защита платёжных операций</li> </ul> <p>Если перечислены все приведённые выше (и, возможно ещё какие-то) - 3 балла          Если перечислены хотя бы 3 - 2 балла          Если приведён хотя бы один - 1 балл</p>
	<b>Общий отзыв к вопросу:</b>	
	<b>Теги:</b>	
<i>Допускает в ответе загрузить файл и/или ввести текст. Ответ должен быть оценен преподавателем вручную.</i>		

### 20.2 Промежуточная аттестация

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в форме устного опроса (индивидуальный опрос, фронтальная беседа, доклады). Критерии оценивания приведены выше.

Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования.

Контрольно-измерительные материалы промежуточной аттестации включают в себя теоретические вопросы, на которые выносятся на обсуждение. Работу студентов на обсуждении позволяет оценить уровень полученных знаний.

Примерный список тем рефератов:

1. Понятие безопасности в современных условиях.
2. Законодательная и нормативно-правовая база защиты информации в РФ.
3. Понятия «модель угроз» и «модель нарушителя».
4. Система сертификации ФСТЭК. (СЗИ НСД СВТ, СЗИ НСД АС. Критерии и т.п.)

5. Классификация систем защиты в Европе и США
6. Межсетевые экраны. Обзор достоинств и недостатков существующих коммерческих и некоммерческих межсетевых экранов
7. Виртуальные частные сети. Обзор достоинств и недостатков существующих средств создания VPN
8. Сетевые системы обнаружения атак. Host-системы обнаружения атак. Обзор достоинств и недостатков существующих средств обнаружения атак.
9. Системы защиты от внутренних атак
10. Вирусы и Антивирусная защита. Обзор существующих антивирусных средств.
11. Биометрия. Принципы, параметры.
12. Криптозащита и криптоанализ
13. Защита почтовых программ, web-трафика и защита от спама.
14. Физическая защита информационных систем от утечки информации
15. Защита настольных и серверных операционных систем.
16. Защита СУБД.
17. Мобильные операционные системы и их защита.
18. Беспроводные технологии и их защита.
19. Облачные системы хранения и обработки. Их защита.
20. Компьютерная криминалистика.
21. Защита интернета вещей.
22. Использование blockchain в системах обмена информацией.
23. Нейроинтерфейсы и сопрягаемое с человеком оборудование.
24. Перспективы и угрозы ИИ

Работы размещаются в системе «Электронный университет» на платформе Moodle и к моменту защиты работы с ней преподаватель и другие студенты могут ознакомиться. На аттестации студент проводит краткую презентацию своей работы и отвечает на вопросы преподавателя и студентов.

При оценивании используются качественные шкалы оценок. Критерии оценивания приведены выше.

Типовые вопросы для оценки усвоения материала:

## Объекты

Основные объекты информационной безопасности:			МС
Балл по умолчанию:			1
Случайный порядок ответов			Да
Нумеровать варианты ответов?			0
Штраф за каждую неправильную попытку:			100
ID-номер:			
#	Ответы	Отзыв	Оценка
A.	Компьютерные сети, базы данных		100
B.	Информационные системы, психологическое состояние пользователей		-100
C.	Бизнес-ориентированные, коммерческие системы		-100
<b>Общий отзыв к вопросу:</b>			
<b>Для любого правильного ответа:</b>		Ваш ответ верный.	
<b>Для любого неправильного ответа:</b>		Ваш ответ неправильный.	
<b>Подсказка 1:</b>			
<b>Показать количество правильных ответов (Подсказка 1):</b>		Нет	
<b>Удалить некорректные ответы (Подсказка 1):</b>		Нет	
<b>Теги:</b>			
Позволяет выбрать один или несколько правильных ответов из заданного списка. (МС/МА)			

## Ответственность

Ответственность за защищенность данных в компьютерной сети несет			МС
Балл по умолчанию:			1
Случайный порядок ответов			Да
Нумеровать варианты ответов?			0
Штраф за каждую неправильную попытку:			100
ID-номер:			
#	Ответы	Отзыв	Оценка
A.	Владелец сети		100
B.	Администратор сети		-100
C.	Пользователь сети		-100
D.	Хакер		-100
Общий отзыв к вопросу:			
Для любого правильного ответа:		Ваш ответ верный.	
Для любого неправильного ответа:		Ваш ответ неправильный.	
Подсказка 1:			
Показать количество правильных ответов (Подсказка 1):		Нет	
Удалить некорректные ответы (Подсказка 1):		Нет	
Теги:			
Позволяет выбирать один или несколько правильных ответов из заданного списка. (МС/МА)			

## Угроза ИС

Угроза информационной системе – это			МС
Балл по умолчанию:			1
Случайный порядок ответов			Да
Нумеровать варианты ответов?			0
Штраф за каждую неправильную попытку:			100
ID-номер:			
#	Ответы	Отзыв	Оценка
A.	Вероятное событие		100
B.	Детерминированное (всегда определенное) событие		-100
C.	Событие, происходящее периодически		-100
<b>Общий отзыв к вопросу:</b>			
<b>Для любого правильного ответа:</b>		Ваш ответ верный.	
<b>Для любого неправильного ответа:</b>		Ваш ответ неправильный.	
<b>Подсказка 1:</b>			
<b>Показать количество правильных ответов (Подсказка 1):</b>		Нет	
<b>Удалить некорректные ответы (Подсказка 1):</b>		Нет	
<b>Теги:</b>			
Позволяет выбирать один или несколько правильных ответов из заданного списка. (МС/МА)			

## Угрозы ИБ

Наиболее распространены угрозы информационной безопасности корпоративной системы		МС	
Балл по умолчанию:		1	
Случайный порядок ответов		Да	
Нумеровать варианты ответов?		0	
Штраф за каждую неправильную попытку:		100	
ID-номер:			
#	Ответы	Отзыв	Оценка
A.	Использование нелегального ПО		-100
B.	Ошибки эксплуатации и неумышленного изменения режима работы системы		100
C.	Сознательного внедрения сетевых вирусов		-100
<b>Общий отзыв к вопросу:</b>			
<b>Для любого правильного ответа:</b>		Ваш ответ верный.	
<b>Для любого неправильного ответа:</b>		Ваш ответ неправильный.	
<b>Подсказка 1:</b>			
<b>Показать количество правильных ответов (Подсказка 1):</b>		Нет	
<b>Удалить некорректные ответы (Подсказка 1):</b>		Нет	
<b>Теги:</b>			
<i>Позволяет выбирать один или несколько правильных ответов из заданного списка. (МС/МА)</i>			

## ЭЦП

Что такое ЭЦП			МА
Балл по умолчанию:			1
Случайный порядок ответов			Да
Нумеровать варианты ответов?			0
Показать количество правильных ответов после окончания:			Да
Штраф за каждую неправильную попытку:			100
ID-номер:			
#	Ответы	Отзыв	Оценка
A.	Электронно-цифровой преобразователь		-50
B.	Электронно-цифровая подпись		100
C.	Электронно-цифровой процессор		-50
<b>Общий отзыв к вопросу:</b>			
<b>Для любого правильного ответа:</b>		Ваш ответ верный.	
<b>Для любого неправильного ответа:</b>		Ваш ответ неправильный.	
<b>Для любого частично правильного ответа:</b>		Ваш ответ частично правильный.	
<b>Подсказка 1:</b>			
<b>Показать количество правильных ответов (Подсказка 1):</b>		Нет	
<b>Удалить некорректные ответы (Подсказка 1):</b>		Нет	
<b>Теги:</b>			
<i>Позволяет выбирать один или несколько правильных ответов из заданного списка. (МС/МА)</i>			



## Длительность восстановления сети.

Команда системных администраторов компании составляет 5 человек. 20 % персонала компании болеет, в отпуске или в командировке.			NUM
Сеть компании насчитывает 400 компьютеров.			
Сколько времени потребуется на восстановление сети после сбоя, в результате которого были выведены из строя 25% компьютеров компании.			
Типичное время сканирования одного компьютера - 1 час,			
Типичное время восстановления повреждённого компьютера - 5 часов.			
ТК не нарушаем; считаем, что и сканирование и восстановление требует полного внимания оператора.			
<b>Балл по умолчанию:</b>			2
<b>Штраф за каждую неправильную попытку:</b>			33.3
<b>ID-номер:</b>			
#	Ответы	Отзыв	Оценка
A.	28.125		100
	<b>Общий отзыв к вопросу:</b>	В рабочих днях	
	<b>Подсказка 1:</b>		
	<b>Показать количество правильных ответов (Подсказка 1):</b>	Нет	
	<b>Удалить некорректные ответы (Подсказка 1):</b>	Нет	
	<b>Теги:</b>		
<i>Импортирование этого типа вопроса не поддерживается.</i>			

## Мощность DDOS-атаки

Рассчитайте мощность DDOS-атаки если в ней используется бот-нет из 50000 устройств посылающих по 1000 запросов с секунду с размером пакета 128 байт.			NUM	
<b>Балл по умолчанию:</b>				1
<b>Штраф за каждую неправильную попытку:</b>				100
<b>ID-номер:</b>				
#	Ответы	Отзыв		Оценка
A.	6.25		100	
	<b>Общий отзыв к вопросу:</b>	В Гбитах в секунду		
	<b>Подсказка 1:</b>			
	<b>Показать количество правильных ответов (Подсказка 1):</b>	Нет		
	<b>Удалить некорректные ответы (Подсказка 1):</b>	Нет		
	<b>Теги:</b>			
<i>Импортирование этого типа вопроса не поддерживается.</i>				

## Открытые точки доступа WI-FI

Опишите риск использования открытых точек доступа Wi-Fi.		ES
<b>Балл по умолчанию:</b>		3
<b>Формат ответа:</b>		HTML-редактор
<b>Требовать текст:</b>		Да
<b>Размер поля:</b>		15
<b>Разрешить вложения:</b>		0
<b>Требуемое число вложений:</b>		0
<b>Разрешенные типы файлов:</b>		
<b>ID-номер:</b>		
	<b>Шаблон ответа</b>	<b>Информация для оценивающих</b>
		<p>В отличном ответе (3 балла) должна быть указана основная проблема - возможность организации злоумышленником фиктивных точек доступа, которые будут выдавать себя за открытую сеть, но при установке соединения смогут собирать весь трафик и все процедуры установки защищённых соединений внутри Wi-fi соединения.</p> <p>В случае, если в ответе будут приведены рассуждения о безопасности Wi-fi, протоколах, их версиях и эти рассуждения будут правильными, то оценка 2</p> <p>В случае, если в ответе будет просто указано, что в этом случае трафик будет не защищён, оценка 1</p>
	<b>Общий отзыв к вопросу:</b>	
	<b>Теги:</b>	
<i>Допускает в ответе загрузить файл и/или ввести текст. Ответ должен быть оценен преподавателем вручную.</i>		

## Функции современных антивирусных решений

Опишите пожалуйста функции современных антивирусных решений. Приведите примеры.		ES
<b>Балл по умолчанию:</b>		3
<b>Формат ответа:</b>		HTML-редактор
<b>Требовать текст:</b>		Да
<b>Размер поля:</b>		15
<b>Разрешить вложения:</b>		0
<b>Требуемое число вложений:</b>		0
<b>Разрешенные типы файлов:</b>		
<b>ID-номер:</b>		
	<b>Шаблон ответа</b>	<b>Информация для оценивающих</b>
		<p>В ответе должны быть отражены</p> <ul style="list-style-type: none"> <li>- кроссплатформенность решения</li> <li>- разнонаправленность решения (контроль файлов, приложений, сетевой активности ... )</li> <li>- менеджер паролей</li> <li>- родительский контроль</li> <li>- защита платёжных операций</li> </ul> <p>Если перечислены все приведённые выше (и, возможно ещё какие-то) - 3 балла          Если перечислены хотя бы 3 - 2 балла          Если приведён хотя бы один - 1 балл</p>
	<b>Общий отзыв к вопросу:</b>	
	<b>Теги:</b>	
<i>Допускает в ответе загрузить файл и/или ввести текст. Ответ должен быть оценен преподавателем вручную.</i>		