

МИНОБРНАУКИ РОССИИ

**Федеральное государственное бюджетное образовательное
учреждение высшего образования "Пермский
государственный национальный исследовательский
университет"**

Кафедра предпринимательства и экономической безопасности

Авторы-составители: **Маринкин Денис Николаевич**

Рабочая программа дисциплины

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КРИПТОЛОГИЯ

Код УМК 64464

Утверждено
Протокол №8
от «24» апреля 2020 г.

Пермь, 2020

1. Наименование дисциплины

Информационная безопасность и криптология

2. Место дисциплины в структуре образовательной программы

Дисциплина входит в обязательную часть Блока « Б.1 » образовательной программы по направлениям подготовки (специальностям):

Направление: **38.03.01** Экономика

направленность "Бухгалтерский учет, анализ и аудит"

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Информационная безопасность и криптология** у обучающегося должны быть сформированы следующие компетенции:

38.03.01 Экономика (направленность : "Бухгалтерский учет, анализ и аудит")

ОПК.2 способность применять современные информационные технологии и программные средства и решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности, использовать различные источники информации по объекту профессиональной деятельности

4. Объем и содержание дисциплины

| | |
|---|--|
| Направления подготовки | 38.03.01 Экономика (направленность: "Бухгалтерский учет, анализ и аудит") |
| форма обучения | заочная |
| №№ триместров, выделенных для изучения дисциплины | 8,9 |
| Объем дисциплины (з.е.) | 3 |
| Объем дисциплины (ак.час.) | 108 |
| Контактная работа с преподавателем (ак.час.), в том числе: | 10 |
| Проведение лекционных занятий | 6 |
| Проведение лабораторных работ, занятий по иностранному языку | 4 |
| Самостоятельная работа (ак.час.) | 98 |
| Формы текущего контроля | Входное тестирование (1) Итоговое контрольное мероприятие (1) Письменное контрольное мероприятие (2) |
| Формы промежуточной аттестации | Зачет (9 триместр) |

5. Аннотированное описание содержания разделов и тем дисциплины

История информационной безопасности и криптологии.

История криптографии: исторические шифры, история отечественной криптографии, средства защиты информации в период перехода от древности к современности, шифры Виженера, модели шифров по К. Шеннону, обобщенная модель шифра, понятие симметричной криптосистемы, системы шифрования с открытыми ключами, блочные и поточные шифры, простейшие шифры и их свойства, композиции шифров, стойкость шифра, однонаправленные функции, современная классификация известных шифров, простые методы криптоанализа известных шифров. Характер криптографической деятельности. Виды информации, подлежащие закрытию, их модели и свойства. Модели нарушителя и безопасных систем. Модель Долева-Яо. Принципы построения криптографических алгоритмов. Понятие криптографического протокола. Протокол Нидхема-Шредера. Понятия аутентификации сущности и аутентификации сообщений. Модели шифров. Основные требования к шифрам. Программные реализации шифров. Особенности использования вычислительной техники в криптографии.

Международные стандарты информационного обмена. Информационная безопасность в условиях функционирования в России глобальных сетей.

Обеспечение международной безопасности жизнедеятельности. Правовые аспекты обеспечения национальной безопасности. Защита трудящихся и охрана труда в системе обеспечения безопасности. Экологическая безопасность. Правовые основы обеспечения безопасности в интернет-среде. Психологические аспекты безопасной коммуникации. Манипуляции в коммуникациях или скрытое психологическое давление. Защищенность в коммуникациях. Личностные характеристики. Информационная безопасность и кибербезопасность. Компьютерный шпионаж и основы защиты информации. Конкурентная разведка и информационно-аналитическая работа в контексте обеспечения безопасности организации.

Правовые основы информационной безопасности и криптологии в России.

Составляющие национальных интересов Российской Федерации в информационной сфере. Понятие, сущность и актуальность защиты информации. Предмет и объект защиты информации. Основные определения и задачи информационной безопасности. Риски и угрозы информационной безопасности. Принципы построения защищенных систем. Нормативно-правовое обеспечение информационной безопасности. Стандарты информационной безопасности. Информация как объект правового регулирования. Информационные правоотношения. Понятие и виды информации, защищаемой законодательством Российской Федерации. Законодательство Российской Федерации в области защиты государственной тайны. Система защиты государственной тайны. Защита интеллектуальной собственности. Защита авторских и смежных прав в законодательстве РФ. Доктрина информационной безопасности Российской Федерации и национальные интересы в информационной сфере. Виды и источники угроз информационной безопасности Российской Федерации. Основные цели и задачи обеспечения информационной безопасности РФ. Правовое обеспечение информационной безопасности РФ. Государственная политика обеспечения информационной безопасности РФ. Государственная система защиты информации Российской Федерации. Международное сотрудничество РФ в области обеспечения информационной безопасности. Угрозы неприкосновенности частной жизни граждан. Кодекс справедливого использования информации. Влияние средств массовой информации на человека.

Виды возможных нарушений информационной системы.

Слухи как социально-психологический феномен. Принятие решений в чрезвычайных ситуациях. Информационные преступления. Основные угрозы безопасности информации. Возможные каналы утечки информации. Основные способы и методы защиты информации. Технологии идентификации

человека. Информационные и психологические войны.

Современные способы защиты информации. Практика их применения.

Методы и технологии защиты информации. Классификация методов и средств защиты информации. Антивирусная защита. Системы идентификации и аутентификации. Системы разграничения доступа. Стеганографические и криптографические методы. Технология электронной подписи. Методы обнаружения и блокирования угроз информационной безопасности. Методы защиты в операционных системах. Сетевые технологии защиты.

Математические основы криптографии. Понятие сложности алгоритма, сложность некоторых известных алгоритмов. Недетерминированное полиномиальное время. Гипотеза $P=NP$. Алгоритм быстрого возведения в степень, обобщенный алгоритм Евклида. Модулярная арифметика. Теоремы Эйлера, Лагранжа, Ферма. Китайская теорема об остатках. Квадратичные вычеты и невычеты. Вычисление квадратного корня в модулярной арифметике по простому и по составному модулям. Понятие о конечных полях по неприводимым многочленам. Методы получения случайных и псевдослучайных последовательностей.

Симметричные криптосистемы. Шифры замены, перестановки, шифры гаммирования. композиционные шифры, сети Файстеля. Блочные шифры: проблема выравнивания, требования к построению блочных шифров. Поточные шифры: синтез поточных шифров, требования к поточным шифрам, режимы использования поточных шифров, синхронизация поточных шифров, опознавание, контроль целостности данных, управление ключами. Криптосистемы DES и отечественного ГОСТа. Стандарт криптографической защиты AES-Rijndael. Криптографическая стойкость шифров. Основные атаки на симметричные шифры. Совершенные шифры. Теоретико-информационный подход к оценке криптостойкости шифров. Вопросы практической стойкости. Имитостойкость и помехоустойчивость шифров. Различие между программными и аппаратными реализациями. Криптографические параметры узлов и блоков шифраторов. Синтез шифров.

Асимметричные криптосистемы. Вопросы организации сетей засекреченной связи. Ключевые системы. Схема открытого распределения ключей Диффи-Хеллмана. K5A. Криптосистема Рабина. криптосистема Эль Гамаль. Сравнение двух классов криптосистем, гибридные криптосистемы. Принципы криптоанализа, критерии распознавания от-крытого текста, универсальные методы криптоанализа: Дифференциальный криптоанализ, дифференциальный криптоанализ DES и трехраундового DES. Битовая стойкость алгоритма RSA. Понятие оракула четности. Битовая стойкость дискретного логарифма.

Криптографические средства контроля целостности. Симметричные средства. Криптографические хеш-функции. Электронная цифровая подпись, цифровая подпись на основе RSA, криптосистемы Рабина и Эль Гамалья. Существующие уязвимости системы Эль-Гамалья.

6. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины требует систематического изучения всех тем в той последовательности, в какой они указаны в рабочей программе.

Основными видами учебной работы являются аудиторские занятия. Их цель - расширить базовые знания обучающихся по осваиваемой дисциплине и систему теоретических ориентиров для последующего более глубокого освоения программного материала в ходе самостоятельной работы. Обучающемуся важно помнить, что контактная работа с преподавателем эффективно помогает ему овладеть программным материалом благодаря расстановке необходимых акцентов и удержанию внимания интонационными модуляциями голоса, а также подключением аудио-визуального механизма восприятия информации.

Самостоятельная работа преследует следующие цели:

- закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;
- формирование навыков подготовки текстовой составляющей информации учебного и научного назначения для размещения в различных информационных системах;
- совершенствование навыков поиска научных публикаций и образовательных ресурсов, размещенных в сети Интернет;
- самоконтроль освоения программного материала.

Обучающемуся необходимо помнить, что результаты самостоятельной работы контролируются преподавателем во время проведения мероприятий текущего контроля и учитываются при промежуточной аттестации.

Обучающимся с ОВЗ и инвалидов предоставляется возможность выбора форм проведения мероприятий текущего контроля, альтернативных формам, предусмотренным рабочей программой дисциплины. Предусматривается возможность увеличения в пределах 1 академического часа времени, отводимого на выполнение контрольных мероприятий.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации.

При проведении текущего контроля применяются оценочные средства, обеспечивающие передачу информации, от обучающегося к преподавателю, с учетом психофизиологических особенностей здоровья обучающихся.

7. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

При самостоятельной работе обучающимся следует использовать:

- конспекты лекций;
- литературу из перечня основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля);
- текст лекций на электронных носителях;
- ресурсы информационно-телекоммуникационной сети "Интернет", необходимые для освоения дисциплины;
- лицензионное и свободно распространяемое программное обеспечение из перечня информационных технологий, используемых при осуществлении образовательного процесса по дисциплине;
- методические указания для обучающихся по освоению дисциплины.

8. Перечень основной и дополнительной учебной литературы

Основная:

1. Информационные технологии в бизнесе. Том 1. Применение системы Decision в микро- и макроэкономике. Учебное пособие: Ай Пи Эр Медиа, 2018. Информационные технологии в бизнесе. Том 1. Применение системы Decision в микро- и макроэкономике / Лихтенштейн В. Е.. - 2018. - 487, ISBN 978-5-4486-0309-9 <http://www.iprbookshop.ru/73871.html>
2. Информационные технологии в бизнесе. Том 2. Применение системы Decision в решении прикладных экономических задач. Учебное пособие: Ай Пи Эр Медиа, 2018. Информационные технологии в бизнесе. Том 2. Применение системы Decision в решении прикладных экономических задач / Лихтенштейн В. Е.. - 2018. - 420, ISBN 978-5-4486-0283-2 <http://www.iprbookshop.ru/73872.html>

Дополнительная:

1. Информационная безопасность и защита информации : учебно-методический комплекс / составители С. А. Омарова, К. А. Исакова, Н. А. Тойганбаева. — Алматы : Нур-Принт, 2012. — 98 с. — ISBN 9965-756-05-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/67055.html>
2. Кудряшев, А. В. Введение в современные веб-технологии : учебное пособие / А. В. Кудряшев, П. А. Светашков. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 359 с. — ISBN 978-5-4497-0313-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/89430.html>

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

<https://solutions.1c.ru/catalog/buhv8/features> 1С Бухгалтерия

www.consultant.ru Консультант плюс

<https://rosstat.gov.ru/> Федеральная служба государственной статистики

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Образовательный процесс по дисциплине **Информационная безопасность и криптология** предполагает использование следующего программного обеспечения и информационных справочных систем:

- 1) презентационные материалы (слайды по темам лекционных занятий);
- 2) доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
- 3) доступ в электронную информационно-образовательную среду университета;
- 4) интернет-сервисы и электронные ресурсы.

Перечень необходимого лицензионного и (или) свободно распространяемого программного обеспечения:

1. Приложения, позволяющее просматривать и воспроизводить медиаконтент PDF-файлов;
2. Офисные пакеты приложений;

При освоении материала и выполнении заданий по дисциплине рекомендуется использование материалов, размещенных в Личных кабинетах обучающихся ЕТИС ПГНИУ (student.psu.ru).

При организации дистанционной работы и проведении занятий в режиме онлайн могут использоваться:

система видеоконференцсвязи на основе платформы BigBlueButton (<https://bigbluebutton.org/>).

система LMS Moodle (<http://e-learn.psu.ru/>), которая поддерживает возможность использования текстовых материалов и презентаций, аудио- и видеоконтент, а так же тесты, проверяемые задания, задания для совместной работы.

система тестирования Indigo (<https://indigotech.ru/>).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

1. Лекционные занятия – аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.
2. Лабораторные занятия – компьютерный класс, оснащенный персональными ЭВМ или аудитория оснащенная презентационной техникой.
3. Самостоятельная работа – аудитория для самостоятельной работы, оснащенная компьютерной техникой с возможностью подключения к сети «Интернет», обеспеченная доступом в электронную информационно-образовательную среду университета. Помещения Научной библиотеки ПГНИУ.
4. Текущий контроль и промежуточная аттестация – аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской

Помещения научной библиотеки ПГНИУ для обеспечения самостоятельной работы обучающихся:

1. Научно-библиографический отдел, корп.1, ауд. 142. Оборудован 3 персональными компьютера с доступом к локальной и глобальной компьютерным сетям.

2. Читальный зал гуманитарной литературы, корп. 2, ауд. 418. Оборудован 7 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

3. Читальный зал естественной литературы, корп.6, ауд. 107а. Оборудован 5 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

4. Отдел иностранной литературы, корп.2 ауд. 207. Оборудован 1 персональным компьютером с доступом к локальной и глобальной компьютерным сетям.

5. Библиотека юридического факультета, корп.9, ауд. 4. Оборудована 11 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

6. Читальный зал географического факультета, корп.8, ауд. 419. Оборудован 6 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

Все компьютеры, установленные в помещениях научной библиотеки, оснащены следующим программным обеспечением:

Операционная система ALT Linux;

Офисный пакет Libreoffice.

Справочно-правовая система «КонсультантПлюс»

**Фонды оценочных средств для аттестации по дисциплине
Информационная безопасность и криптология**

**Планируемые результаты обучения по дисциплине для формирования компетенции.
Индикаторы и критерии их оценивания**

ОПК.2

способность применять современные информационные технологии и программные средства и решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности, использовать различные источники информации по объекту профессиональной деятельности

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|---|---|---|
| <p>ОПК.2 способность применять современные информационные технологии и программные средства и решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности, использовать различные источники информации по объекту профессиональной деятельности</p> | <p>Знать:основы организации современных ЭВМ и их общие характеристики, тенденции развития устройств компьютера и компьютерных сетей, принципы организации использования средств вычислительной техники Уметь:применять информационно-коммуникационные технологии при решении стандартных задач профессиональной деятельности Владеть:основными методами решения проблем информационной безопасности компьютерных систем и защиты информации</p> | <p align="center">Неудовлетворител</p> <p>не знает:основы организации современных ЭВМ и их общие характеристики, тенденции развития устройств компьютера и компьютерных сетей, принципы организации использования средств вычислительной техники не умеет:применять информационно-коммуникационные технологии при решении стандартных задач профессиональной деятельности не владеет:основными методами решения проблем информационной безопасности компьютерных систем и защиты информации</p> <p align="center">Удовлетворительн</p> <p>общие но не структурированные знания:основ организации современных ЭВМ и их общих характеристик, тенденции развития устройств компьютера и компьютерных сетей, принципы организации использования средств вычислительной техники частично сформированное умение:применять информационно-коммуникационные технологии при решении стандартных задач профессиональной деятельности фрагментарное владение:основными методами решения проблем информационной безопасности</p> |

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|----------------------------|------------------------------------|--|
| | | <p style="text-align: center;">Удовлетворительн</p> <p>компьютерных систем и защиты информации</p> <p style="text-align: center;">Хорошо</p> <p>сформированные но содержащие пробелы знания:основ организации современных ЭВМ и их общих характеристик, тенденции развития устройств компьютера и компьютерных сетей, принципы организации использования средств вычислительной техники</p> <p>успешные но содержащие пробелы умения применять информационно-коммуникационные технологии при решении стандартных задач профессиональной деятельности</p> <p>успешное но содержащее пробелы владение:основными методами решения проблем информационной безопасности компьютерных систем и защиты информации</p> <p style="text-align: center;">Отлично</p> <p>сформированные систематические знания основ организации современных ЭВМ и их общих характеристик, тенденции развития устройств компьютера и компьютерных сетей, принципы организации использования средств вычислительной техники</p> <p>сформированное умение применять информационно-коммуникационные технологии при решении стандартных задач профессиональной деятельности</p> <p>успешное владение основными методами решения проблем информационной безопасности компьютерных систем и защиты информации</p> |

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : заочное_2019

Вид мероприятия промежуточной аттестации : Не предусмотрено

| Компетенция (индикатор) | Мероприятие текущего контроля | Контролируемые элементы результатов обучения |
|---|--|--|
| Входной контроль | История информационной безопасности и криптологии. Входное тестирование | знает историю криптографии. владеет современной классификацией известных шифров, простых методов криптоанализа известных шифров. различает виды информации, подлежащие закрытию, их модели и свойства. владеет понятием криптографического протокола. различает особенности использования вычислительной техники в криптографии. |
| ОПК.2 способность применять современные информационные технологии и программные средства и решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности, использовать различные источники информации по объекту профессиональной деятельности | Правовые основы информационной безопасности и криптологии в России. Письменное контрольное мероприятие | Знает нормативно-правовое обеспечение информационной безопасности, стандарты информационной безопасности. умеет дать определение информационным правоотношениям. различает виды информации, защищаемой законодательством Российской Федерации. Знает Законодательство Российской Федерации в области защиты государственной тайны. Знает систему защиты государственной тайны. понимает что такое защита авторских и смежных прав в законодательстве РФ. |

Спецификация мероприятий текущего контроля

История информационной безопасности и криптологии.

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **0**

Проходной балл: **0**

| Показатели оценивания | Баллы |
|--|-------|
| знает историю криптографии. владеет современной классификацией известных шифров, | 10 |

| | |
|---|-----|
| простых методов криптоанализа известных шифров. различает виды информации, подлежащие закрытию, их модели и свойства. владеет понятием криптографического протокола. различает особенности использования вычислительной техники в криптографии. | |
| знает историю криптографии. владеет современной классификацией известных шифров, простых методов криптоанализа известных шифров. различает виды информации, подлежащие закрытию, их модели и свойства. | 7 |
| знает историю криптографии. владеет современной классификацией известных шифров, простых методов криптоанализа известных шифров. | 5 |
| не знает историю криптографии. не владеет современной классификацией известных шифров, простых методов криптоанализа известных шифров. не различает виды информации, подлежащие закрытию, их модели и свойства. не владеет понятием криптографического протокола. не различает особенности использования вычислительной техники в криптографии. 4.5 Записи с 1 по 4 | 4.5 |

Правовые основы информационной безопасности и криптологии в России.

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**

Проходной балл: **13**

| Показатели оценивания | Баллы |
|--|--------------|
| Знает нормативно-правовое обеспечение информационной безопасности, стандарты информационной безопасности. умеет дать определение информационным правоотношениям. различает виды информации, защищаемой законодательством Российской Федерации. Знает Законодательство Российской Федерации в области защиты государственной тайны. Знает систему защиты государственной тайны. понимает что такое защита авторских и смежных прав в законодательстве РФ. | 30 |
| Знает нормативно-правовое обеспечение информационной безопасности, стандарты информационной безопасности. Знает Законодательство Российской Федерации в области защиты государственной тайны. Знает систему защиты государственной тайны. понимает что такое защита авторских и смежных прав в законодательстве РФ. | 20 |
| Знает нормативно-правовое обеспечение информационной безопасности, стандарты информационной безопасности. умеет дать определение информационным правоотношениям. различает виды информации, защищаемой законодательством Российской Федерации. | 13 |
| не знает нормативно-правовое обеспечение информационной безопасности, стандарты информационной безопасности. не умеет дать определение информационным правоотношениям. не различает виды информации, защищаемой законодательством Российской Федерации. не знает Законодательство Российской Федерации в области защиты государственной тайны. не знает систему защиты государственной тайны. не понимает что такое защита авторских и смежных прав в законодательстве РФ. | 12 |

Вид мероприятия промежуточной аттестации : Зачет

Способ проведения мероприятия промежуточной аттестации : Оценка по дисциплине в рамках промежуточной аттестации определяется на основе баллов, набранных обучающимся на контрольных мероприятиях, проводимых в течение учебного периода.

Максимальное количество баллов : 100

Конвертация баллов в отметки

«отлично» - от 81 до 100

«хорошо» - от 61 до 80

«удовлетворительно» - от 44 до 60

«неудовлетворительно» / «незачтено» менее 44 балла

| Компетенция (индикатор) | Мероприятие текущего контроля | Контролируемые элементы результатов обучения |
|---|--|--|
| ОПК.2 способность применять современные информационные технологии и программные средства и решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности, использовать различные источники информации по объекту профессиональной деятельности | Современные способы защиты информации. Практика их применения. Письменное контрольное мероприятие | Знает методы и технологии защиты информации. различает классификацию методов и средств защиты информации. Знает что такое антивирусная защита. владеет системой идентификации и аутентификации. владеет методами обнаружения и блокирования угроз информационной безопасности. знает сетевые технологии защиты. |

| Компетенция (индикатор) | Мероприятие текущего контроля | Контролируемые элементы результатов обучения |
|---|--|--|
| ОПК.2 способность применять современные информационные технологии и программные средства и решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности, использовать различные источники информации по объекту профессиональной деятельности | Итоговый контроль по дисциплине Итоговое контрольное мероприятие | Знает историю информационной безопасности и криптологии. владеет правовыми основами информационной безопасности и криптологии в России. различает виды возможных нарушений информационной системы, владеет современными способами защиты информации. |

Спецификация мероприятий текущего контроля

Современные способы защиты информации. Практика их применения.

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**

Проходной балл: **13**

| Показатели оценивания | Баллы |
|---|-------|
| Знает методы и технологии защиты информации. различает классификацию методов и средств защиты информации. Знает что такое антивирусная защита. владеет системой идентификации и аутентификации. владеет методами обнаружения и блокирования угроз информационной безопасности. знает сетевые технологии защиты. | 30 |
| Знает методы и технологии защиты информации. различает классификацию методов и средств защиты информации. Знает что такое антивирусная защита. владеет системой идентификации и аутентификации. | 20 |
| Знает методы и технологии защиты информации. различает классификацию методов и средств защиты информации. Знает что такое антивирусная защита. | 13 |
| не знает методы и технологии защиты информации. не различает классификацию методов и средств защиты информации. не знает что такое антивирусная защита. не владеет системой идентификации и аутентификации. не владеет методами обнаружения и блокирования угроз информационной безопасности. не знает сетевые технологии защиты. | 12 |

Итоговый контроль по дисциплине

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**

Проходной балл: **18**

| Показатели оценивания | Баллы |
|--|--------------|
| Знает историю информационной безопасности и криптологии.владеет правовыми основами информационной безопасности и криптологии в России.различает виды возможных нарушений информационной системы, владеет современными способами защиты информации. | 40 |
| владеет правовыми основами информационной безопасности и криптологии в России. различает виды возможных нарушений информационной системы, владеет современными способами защиты информации. | 30 |
| Знает историю информационной безопасности и криптологии.владеет правовыми основами информационной безопасности и криптологии в России. | 18 |
| не знает историю информационной безопасности и криптологии.не владеет правовыми основами информационной безопасности и криптологии в России.не различает виды возможных нарушений информационной системы, не владеет современными способами защиты информации. | 17 |