

МИНОБРНАУКИ РОССИИ

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

Кафедра информационной безопасности и систем связи

**Авторы-составители: Бячкова Наталия Борисовна
Черников Арсений Викторович**

Рабочая программа дисциплины

ПСИХОЛОГИЧЕСКИЕ СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Код УМК 69473

**Утверждено
Протокол №1
от «31» августа 2020 г.**

Пермь, 2020

1. Наименование дисциплины

Психологические средства и методы защиты информации

2. Место дисциплины в структуре образовательной программы

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

Специальность: **10.05.01** Компьютерная безопасность

направленность Разработка защищенного программного обеспечения

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Психологические средства и методы защиты информации** у обучающегося должны быть сформированы следующие компетенции:

10.05.01 Компьютерная безопасность (направленность : Разработка защищенного программного обеспечения)

ОПК.6 способность понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства

ПК.5 Способность осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций

ПК.7 Способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований

ПК.8 Способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем, а также положений, инструкций и других организационно-распорядительных документов

ПК.10 Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах

ПК.16 способность организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности

ПК.17 Способность разрабатывать планы работы первичных подразделений

ПК.18 способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы

4. Объем и содержание дисциплины

| | |
|---|--|
| Направления подготовки | 10.05.01 Компьютерная безопасность (направленность: Разработка защищенного программного обеспечения) |
| форма обучения | очная |
| №№ триместров, выделенных для изучения дисциплины | 13,14 |
| Объем дисциплины (з.е.) | 6 |
| Объем дисциплины (ак.час.) | 216 |
| Контактная работа с преподавателем (ак.час.), в том числе: | 84 |
| Проведение лекционных занятий | 28 |
| Проведение лабораторных работ, занятий по иностранному языку | 56 |
| Самостоятельная работа (ак.час.) | 132 |
| Формы текущего контроля | Итоговое контрольное мероприятие (2) Письменное контрольное мероприятие (13) |
| Формы промежуточной аттестации | Зачет (13 триместр) Экзамен (14 триместр) |

5. Аннотированное описание содержания разделов и тем дисциплины

Психологические средства и методы защиты информации. Первый семестр

Понятие информационно-психологической угрозы. Роль человеческого фактора в политике безопасности предприятия. Способы и приемы организации безопасного менеджмента, воздействия на корпоративную культуру и динамику организации.

Корпоративная культура организации в информационной политике организации

Понятие информационно-психологической угрозы. Роль человеческого фактора в политике безопасности предприятия. Обзор основных способов и приемов противостояния психологическому и информационному воздействию

Психологические средства и методы защиты информации в сфере организационной культуры

Понятие информационно-психологической угрозы. Роль человеческого фактора в политике безопасности предприятия

Практика применения психологических средств и методов защиты информации в сфере организационной культуры

Обзор основных способов и приемов противостояния психологическому и информационному воздействию

Психологические средства и методы защиты информации в реализации управленческого цикла

Способы и приемы организации безопасного менеджмента, воздействия на корпоративную культуру и динамику организации.

Психологические средства и методы защиты информации в сфере деятельностно-административных функций управления

Понятие корпоративной культуры. Типичные информационно-психологические угрозы в корпоративной культуре предприятия. Воздействие на корпоративную культуру.

Практика применения психологических средств и методов защиты информации в сфере деятельностно-административных функций управления

Система управленческих функций предприятия. Информационно-психологические угрозы в сфере менеджмента. Способы и приемы организации безопасного менеджмента.

Психологические средства и методы защиты информации в сфере организационных коммуникаций

Безопасность динамики организации. Управление групповыми процессами и состояниями. Создание безопасной ролевой структуры организации

Психологические средства и методы защиты информации в мотивационной сфере персонала и системе стимулирования организации

Способы стимулирования персонала. Группы риска в сфере трудовой мотивации. Способы коррекции негативных явлений в сфере трудовой мотивации

Практика применения психологических средств и методов защиты информации в мотивационной сфере персонала и системе стимулирования организации

Диагностика угроз в сфере трудовой мотивации сотрудников. Разработка профилактических и коррекционных мероприятий с целью снижения угроз в сфере трудовой мотивации сотрудников

Профилактика и коррекция негативных социально-психологических явлений в системе информационной безопасности организации

Владение системой знаний в сфере профилактики и коррекции угроз со стороны человеческого фактора в системе информационной безопасности организации

Психологические средства и методы защиты информации. Второй семестр

Воздействие на трудовую мотивацию персонала. Профилактика угроз в информационном обмене предприятия. Способы и приемы профилактики угроз в работе с персоналом. Конфликт в политике безопасности предприятия. Управление конфликтами.

Психологические средства и методы защиты информации в системе развития организации

Воздействие на трудовую мотивацию персонала. Профилактика угроз в информационном обмене предприятия. Способы и приемы профилактики угроз в работе с персоналом. Конфликт в политике безопасности предприятия. Управление конфликтами.

Психологические средства и методы защиты информации в сфере групповой динамики организации.

Понятие безопасной трудовой мотивации. Группы риска в трудовой мотивации.

Практика применения психологических средств и методов защиты информации в сфере групповой динамики организации

Дифференцированный подход к стимулированию сотрудников. Воздействие на трудовую мотивацию персонала.

Психологические средства и методы защиты информации в сфере конфликтного взаимодействия сотрудников организации

Безопасность организационных коммуникаций. Оптимизация коммуникативного процесса. Профилактика угроз в информационном обмене предприятия.

Практика применения психологических средств и методов защиты информации в сфере конфликтного взаимодействия сотрудников организации

Безопасность кадровой политики. Основные кадровые технологии. Способы и приемы профилактики угроз в работе с персоналом.

Психологические средства и методы защиты информации в сфере кадровой политики организации

Конфликт в политике безопасности предприятия. Управление конфликтами.

Практика применения психологических средств и методов защиты информации в сфере кадровой политики организации

Диагностика угроз в сфере кадровой политики. Разработка рекомендаций с целью профилактики и коррекции угроз в сфере кадровой политики

Организация системы информационной безопасности организации

Владение системой знаний в сфере профилактики и коррекции угроз со стороны человеческого фактора в системе информационной безопасности организации

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 аудиторные 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. Бячкова Н. Б. Психологические особенности профессиональной деятельности: личностные особенности сотрудников как фактор информационной безопасности: учебно-методическое пособие для студентов, обучающихся по направлению подготовки бакалавров «Экономическая безопасность» и по специальностям «Компьютерная безопасность», «Информационная безопасность автоматизированных систем»/Н. Б. Бячкова.-Пермь:ПГНИУ,2020, ISBN 978-5-7944-3564-1.-106. <https://elis.psu.ru/node/638544>

Дополнительная:

1. Бячкова Н. Б. Основы безопасности управленческой деятельности: учебное пособие/Н. Б. Бячкова.- Пермь,2014, ISBN 978-5-7944-2347-1.-242.-Библиогр.: с. 240-241

2. Трунов Д. Г. Организационная конфликтология: лекции : методическое пособие для студентов вузов/Д. Г. Трунов.-Пермь:[ПГУ],2008.-74.-Библиогр.: с. 73

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

<http://www.psu.ru/elektronnye-resursy-dlya-psu> Электронные ресурсы для ПГНИУ

<http://www.mathnet.ru/> Общероссийский математический портал

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

Образовательный процесс по дисциплине **Психологические средства и методы защиты информации** предполагает использование следующего программного обеспечения и информационных справочных систем:

Образовательный процесс по дисциплине предполагает использование следующего программного обеспечения и информационных справочных систем:

- доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
- доступ в электронную информационно-образовательную среду университета.

Необходимое лицензионное и (или) свободно распространяемое программное обеспечение:

- приложение позволяющее просматривать и воспроизводить медиаконтент PDF-файлов «Adobe Acrobat Reader DC»;
- офисный пакет приложений «LibreOffice», Alt Linux.

При освоении материала и выполнения 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

Для лекционных занятий требуется аудитория, оснащенная презентационной техникой (проектором и т.д.); экран для проектора, маркерная или меловая доска, компьютер/ноутбук.

Для лабораторных работ требуется аудитория Лаборатории Информационной безопасности: аппаратные и программные средства определены паспортом лаборатории.

Для самостоятельной работы требуется аудитория помещения Научной библиотеки ПГНИУ, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет», обеспеченные доступом в электронную информационно-образовательную среду университета и с доступом к ЭБС.

Помещения научной библиотеки ПГНИУ для обеспечения самостоятельной работы обучающихся:

1. Научно-библиографический отдел, корп.1, ауд. 142. Оборудован 3 персональными компьютерами 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
Психологические средства и методы защиты информации**

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

ОПК.6

способность понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|---|--|---|
| ОПК.6 способность понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства | Умеет понимать социальную значимость своей будущей профессии, цели и смысл государственной службы. Владеет высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства. | <p style="text-align: center;">Неудовлетворител</p> Не умеет анализировать социальные ситуации в сфере информационной безопасности, не знает способы и приемы самомотивирования,, навык применения дифференцированного подхода в стимулировании персонала не сформирован <p style="text-align: center;">Удовлетворительн</p> Допускает негрубые ошибки в анализе социальных ситуаций в сфере информационной безопасности, в целом знает способы и приемы самомотивирования,, навык применения дифференцированного подхода в стимулировании персонала в целом сформирован <p style="text-align: center;">Хорошо</p> Допускает отдельные неточности в анализе социальных ситуаций в сфере информационной безопасности, в целом знает способы и приемы самомотивирования,, навык применения дифференцированного подхода в стимулировании персонала в целом сформирован <p style="text-align: center;">Отлично</p> Анализирует социальные ситуации в сфере информационной безопасности без ошибок, в целом знает способы и приемы самомотивирования,, навык применения дифференцированного подхода в стимулировании персонала |

ПК.5

Способность осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|--|---|--|
| ПК.5 Способность осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций | Умеет осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем. Владеет навыками передачи результатов проведенных исследований в виде конкретных рекомендаций по профилактике и коррекции негативных явлений в сфере управления человеческим фактором. | <p>Неудовлетворител Компетенция не сформирована</p> <p>Удовлетворительн При составлении аналитических обзоров имеет представление о роли человеческого фактора в информационной безопасности компьютерных систем. Способен в целом сформулировать меры профилактики и коррекции в сфере корпоративной культуры предприятия, реализации управленческого цикла, реализации кадровой политики, динамики группы, организационных коммуникаций</p> <p>Хорошо При составлении аналитических обзоров объясняет роль человеческого фактора в информационной безопасности компьютерных систем. Допускает неточности в формулировании мер профилактики и коррекции в сфере корпоративной культуры предприятия, реализации управленческого цикла, реализации кадровой политики, динамики группы, организационных коммуникаций</p> <p>Отлично При составлении аналитических обзоров аргументированно объясняет роль человеческого фактора в информационной безопасности компьютерных систем. Обладает навыками в формулировании мер профилактики и коррекции в сфере корпоративной культуры предприятия, реализации управленческого цикла, реализации кадровой политики, динамики группы, организационных коммуникаций</p> |

ПК.7

Способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|--|--|---|
| ПК.7 Способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований | Умеет проводить обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом знаний особенностей реализации управленческого цикла, особенностей трудовой мотивации персонала. Знает влияние особенностей корпоративной культуры, организационного развития на обоснование и выбор рационального решения. | Неудовлетворител Компетенция не сформирована Удовлетворительн Имеет представление об обосновании и выборе рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом знаний особенностей реализации управленческого цикла, особенностей трудовой мотивации персонала. Имеет представление о влиянии особенностей корпоративной культуры, организационного развития на обоснование и выбор рационального решения Хорошо Допускает отдельные неточности в обосновании и выборе рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом знаний особенностей реализации управленческого цикла, особенностей трудовой мотивации персонала. Сформированы знания о влиянии особенностей корпоративной культуры, организационного развития на обоснование и выбор рационального решения Отлично Владеет навыками обоснования и выбора рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом знаний особенностей реализации управленческого цикла, особенностей трудовой мотивации персонала. Владеет навыком использования особенностей корпоративной культуры, организационного развития при обосновании и выборе рационального решения |

ПК.17

Способность разрабатывать планы работы первичных подразделений

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|--|--|--|
| ПК.17 Способность разрабатывать планы работы первичных подразделений | Умеет разрабатывать планы работы первичных подразделений с учетом знаний по реализации принципов оптимального планирования. Знает влияние групповых процессов и состояний, групповых эффектов на реализацию функции планирования. Владеет навыками планирования деятельности первичных подразделений особенности корпоративной культуры, уровень конфликтности группы. | <p>Неудовлетворител Компетенция не сформирована</p> <p>Удовлетворительн В целом владеет способами разработки планов работы первичных подразделений с учетом принципов оптимального планирования. Имеет представление о влиянии групповых процессов и состояний, групповых эффектов на реализацию функции планирования. Допускает неточности при учитывании в планировании деятельности первичных подразделений особенностей корпоративной культуры, уровня конфликтности группы</p> <p>Хорошо Владеет способами разработки планов работы первичных подразделений с учетом принципов оптимального планирования. Имеет знания о влиянии групповых процессов и состояний, групповых эффектов, особенностей корпоративной культуры, уровня конфликтности группы на реализацию функции планирования. Допускает отдельные неточности.</p> <p>Отлично Свободно владеет способами разработки планов работы первичных подразделений с учетом принципов оптимального планирования. Имеет прочные знания о влиянии групповых процессов и состояний, групповых эффектов, особенностей корпоративной культуры, уровня конфликтности группы на реализацию функции планирования. Не допускает ошибок и неточностей.</p> |
| ПК.17 Способность разрабатывать планы работы первичных подразделений | Умеет разрабатывать планы работы первичных подразделений с учетом особенностей управленческого цикла и корпоративной культуры предприятия, мотивации персонала, уровня развития группы, кадровой | <p>Неудовлетворител Компетенция не сформирована</p> <p>Удовлетворительн Допускает отдельные ошибки при разработке планов работы первичных подразделений с учетом особенностей управленческого цикла и корпоративной культуры предприятия, мотивации</p> |

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|----------------------------|------------------------------------|--|
| | ситуации в организации. | <p>Удовлетворительн персонала, уровня развития группы, кадровой ситуации в организации</p> <p>Хорошо Умеет разрабатывать планы работы первичных подразделений с учетом особенностей управленческого цикла и корпоративной культуры предприятия, мотивации персонала, уровня развития группы, кадровой ситуации в организации. Допускает отдельные неточности</p> <p>Отлично Владеет навыком разработки планов работы первичных подразделений с учетом особенностей управленческого цикла и корпоративной культуры предприятия, мотивации персонала, уровня развития группы, кадровой ситуации в организации</p> |

ПК.8

Способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем, а также положений, инструкций и других организационно-распорядительных документов

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|---|---|---|
| ПК.8 Способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем, а также положений, инструкций и других организационно-распорядительных документов | Умеет разрабатывать проекты нормативных и методических материалов, регламентирующих организационные отношения с целью обеспечения информационной безопасности компьютерных систем, а также положений, инструкций и других организационно-распорядительных документов. Знает основы информационной безопасности. | <p>Неудовлетворител Компетенция не сформирована</p> <p>Удовлетворительн Допускает отдельные ошибки при разработке проектов нормативных и методических материалов, регламентирующих организационные отношения с целью обеспечения информационной безопасности компьютерных систем, а также положений, инструкций и других организационно-распорядительных документов</p> <p>Хорошо Умеет разрабатывать, но допускает отдельные неточности проекты нормативных и методических материалов, регламентирующих организационные отношения с целью обеспечения информационной безопасности</p> |

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|----------------------------|------------------------------------|--|
| | | <p>Хорошо компьютерных систем, а также положений, инструкций и других организационно-распорядительных документов</p> <p>Отлично Владеет навыком разработки проектов нормативных и методических материалов, регламентирующих организационные отношения с целью обеспечения информационной безопасности компьютерных систем, а также положений, инструкций и других организационно-распорядительных документов</p> |

ПК.10

Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|--|---|---|
| <p>ПК.10 Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах</p> | <p>Знает основы информационной безопасности. Умеет участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах посредством эффективной реализации деятельностно-административных функций управления и кадровой политики. Знает способы и приемы воздействия на корпоративную культуру предприятия, динамику организационного развития, систему организационных коммуникаций, трудовую мотивацию персонала.</p> | <p>Неудовлетворител компетенция не сформирована</p> <p>Удовлетворительн в целом знает способы и приемы разработки системы защиты информации, основные направления реализации управленческих функций, методы управления мотивацией сотрудников, организации кадровой политики на предприятии</p> <p>Хорошо знает особенности разработки системы защиты информации, основные направления реализации управленческих функций с учетом особенностей реализации управленческого цикла, корпоративной культуры, спецификой управления трудовой мотивацией, динамикой организации и организацией кадровой политики, умеет разрабатывать формальные модели политик безопасности</p> <p>Отлично умеет диагностировать угрозы в системе защиты информации с учетом управления человеческим фактором, умеет</p> |

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|----------------------------|------------------------------------|---|
| | | <p>Отлично</p> <p>разрабатывать формальные модели политик безопасности с учетом применения методов воздействия на корпоративную культуру, трудовую мотивацию, динамику организации и кадровую политику, владеет навыками формулирования рекомендаций по коррекции негативных явлений, связанных с человеческим фактором в сфере системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы и политик безопасности</p> |

ПК.16

способность организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|--|--|---|
| <p>ПК.16</p> <p>способность организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности</p> | <p>Умеет организовывать работу малых коллективов исполнителей. Умеет воздействовать на развитие малой группы, находить и принимать управленческие решения в сфере профессиональной деятельности с целью минимизации угроз, связанных с человеческим фактором. Умеет учитывать при организации работы малых коллективов особенности организационных коммуникаций, корпоративной культуры, уровень конфликтности коллектива, особенности трудовой мотивации и динамики группы.</p> | <p>Неудовлетворител компетенция не сформирована</p> <p>Удовлетворительн в целом знает основные направления организации работы малой группы посредством снижения уровня угроз для информационной безопасности в сфере корпоративной культуры, трудовой мотивации, динамики малой группы, конфликтности группы, организационных коммуникациях</p> <p>Хорошо умеет диагностировать различные негативные явления в организации работы малой группы, знает особенности корпоративных культур на российских предприятиях, владеет способами и приемами воздействия на корпоративную культуру, трудовую мотивацию, динамику малой группы, уровень конфликтности группы, организационные коммуникации с целью снижения уровня угроз для информационной безопасности</p> <p>Отлично свободно владеет навыками выявления угроз в организации работы малой группы, в</p> |

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|----------------------------|------------------------------------|--|
| | | <p>Отлично</p> <p>корпоративной культуре, умеет формулировать рекомендации по коррекции негативных явлений в работе малой группы, корпоративной культуре предприятия, трудовой мотивации, динамике малой группы, уровне конфликтности группы, организационных коммуникациях</p> |

ПК.18

способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|--|---|---|
| <p>ПК.18</p> <p>способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы</p> | <p>Умеет разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы. Знает основы информационной безопасности.</p> | <p>Неудовлетворител</p> <p>Не знает способы и приемы совершенствования системы организационных коммуникаций, не владеет навыков разработки коррекционных и профилактических программ</p> <p>Удовлетворительн</p> <p>Знает способы и приемы совершенствования системы организационных коммуникаций, владеет навыков разработки коррекционных и профилактических программ, допуская негрубые ошибки</p> <p>Хорошо</p> <p>В целом знает способы и приемы совершенствования системы организационных коммуникаций, владеет навыков разработки коррекционных и профилактических программ, допуская отдельные неточности</p> <p>Отлично</p> <p>Знает способы и приемы совершенствования системы организационных коммуникаций, владеет навыков разработки коррекционных и профилактических программ на высоком уровне</p> |

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : СУОС

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 48 до 60

«неудовлетворительно» / «незачтено» менее 48 балла

| Компетенция (индикатор) | Мероприятие текущего контроля | Контролируемые элементы результатов обучения |
|------------------------------------|--|---|
|------------------------------------|--|---|

| Компетенция (индикатор) | Мероприятие текущего контроля | Контролируемые элементы результатов обучения |
|--|--|---|
| <p>ОПК.6 способность понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства</p> <p>ПК.8 Способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем, а также положений, инструкций и других организационно-распорядительных документов</p> <p>ПК.16 способность организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности</p> <p>ПК.17 Способность разрабатывать планы работы первичных подразделений</p> | <p>Психологические средства и методы защиты информации в сфере организационной культуры</p> <p>Письменное контрольное мероприятие</p> | <p>Коллоквиум "Безопасность организационной культуры"</p> |

| Компетенция (индикатор) | Мероприятие текущего контроля | Контролируемые элементы результатов обучения |
|--|--|---|
| <p>ПК.5 Способность осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций</p> <p>ПК.7 Способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований</p> <p>ПК.8 Способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем, а также положений, инструкций и других организационно-распорядительных документов</p> <p>ПК.10 Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах</p> <p>ПК.16 способность организовывать работу малых коллективов исполнителей, находить и принимать управленческие</p> | <p>Практика применения психологических средств и методов защиты информации в сфере организационной культуры</p> <p>Письменное контрольное мероприятие</p> | <p>Письменная лабораторная работа</p> |

| Компетенция (индикатор) | Мероприятие текущего контроля | Контролируемые элементы результатов обучения |
|--|--|---|
| <p>решения в сфере профессиональной деятельности</p> <p>ПК.17</p> <p>Способность разрабатывать планы работы первичных подразделений</p> | | |
| <p>ПК.17</p> <p>Способность разрабатывать планы работы первичных подразделений</p> | <p>Психологические средства и методы защиты информации в сфере деятельности - административных функций управления</p> <p>Письменное контрольное мероприятие</p> | <p>Письменная контрольная работа</p> |

| Компетенция (индикатор) | Мероприятие текущего контроля | Контролируемые элементы результатов обучения |
|--|--|---|
| <p>ПК.5 Способность осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций</p> <p>ПК.7 Способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований</p> <p>ПК.8 Способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем, а также положений, инструкций и других организационно-распорядительных документов</p> <p>ПК.10 Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах</p> <p>ПК.16 способность организовывать работу малых коллективов исполнителей, находить и принимать управленческие</p> | <p>Практика применения психологических средств и методов защиты информации в сфере деятельности - административных функций управления</p> <p>Письменное контрольное мероприятие</p> | <p>Письменная лабораторная работа</p> |

| Компетенция (индикатор) | Мероприятие текущего контроля | Контролируемые элементы результатов обучения |
|---|--|---|
| <p>решения в сфере профессиональной деятельности</p> <p>ПК.17</p> <p>Способность разрабатывать планы работы первичных подразделений</p> | | |
| <p>ПК.7</p> <p>Способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований</p> <p>ПК.17</p> <p>Способность разрабатывать планы работы первичных подразделений</p> | <p>Психологические средства и методы защиты информации в сфере организационных коммуникаций</p> <p>Письменное контрольное мероприятие</p> | <p>Письменная контрольная работа</p> |
| <p>ПК.7</p> <p>Способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований</p> <p>ПК.10</p> <p>Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах</p> | <p>Психологические средства и методы защиты информации в мотивационной сфере персонала и системе стимулирования организации</p> <p>Письменное контрольное мероприятие</p> | <p>Коллоквиум</p> |

| Компетенция (индикатор) | Мероприятие текущего контроля | Контролируемые элементы результатов обучения |
|--|--|---|
| <p>ПК.7 Способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований</p> <p>ПК.16 способность организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности</p> <p>ПК.18 способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы</p> | <p>Практика применения психологических средств и методов защиты информации в мотивационной сфере персонала и системе стимулирования организации</p> <p>Письменное контрольное мероприятие</p> | <p>Письменная лабораторная работа</p> |

| Компетенция (индикатор) | Мероприятие текущего контроля | Контролируемые элементы результатов обучения |
|--|---|---|
| <p>ПК.5 Способность осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций</p> <p>ПК.7 Способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований</p> <p>ПК.8 Способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем, а также положений, инструкций и других организационно-распорядительных документов</p> <p>ПК.10 Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах</p> <p>ПК.16 способность организовывать работу малых коллективов исполнителей, находить и принимать управленческие</p> | <p>Профилактика и коррекция негативных социально - психологических явлений в системе информационной безопасности организации</p> <p>Итоговое контрольное мероприятие</p> | <p>Письменная контрольная работа</p> |

| Компетенция (индикатор) | Мероприятие текущего контроля | Контролируемые элементы результатов обучения |
|---|--|---|
| решения в сфере профессиональной деятельности ПК.17 Способность разрабатывать планы работы первичных подразделений | | |

Спецификация мероприятий текущего контроля

Психологические средства и методы защиты информации в сфере организационной культуры

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**

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

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **10**

Проходной балл: **5**

| Показатели оценивания | Баллы |
|--|--------------|
| Умеет анализировать влияние корпоративной культуры на информационную безопасность организации. Владеет способами диагностики вида корпоративной культуры | 4 |
| Способен применять приемы профилактики негативных явлений в сфере корпоративной культуры | 3 |
| Знает понятия в сфере корпоративной культуры: уровни, элементы культуры, толщина культуры, типы культуры | 3 |

Практика применения психологических средств и методов защиты информации в сфере организационной культуры

Продолжительность проведения мероприятия промежуточной аттестации: **6 часа**

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

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **10**

Проходной балл: **5**

| Показатели оценивания | Баллы |
|---|--------------|
| Разработка профилактических и коррекционных мероприятий с целью минимизации угроз со стороны человеческого фактора в сфере организационной культуры | 5 |
| Диагностика угроз в сфере организационной культуры | 5 |

Психологические средства и методы защиты информации в сфере деятельности - административных функций управления

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**

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

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **10**

Проходной балл: **5**

| Показатели оценивания | Баллы |
|---|--------------|
| Разработка профилактических и коррекционных мероприятий с целью минимизации угроз | 5 |

| | |
|--|---|
| со стороны человеческого фактора в сфере деятельностно-административных функций управления | |
| Диагностика угроз со стороны человеческого фактора в сфере деятельностно-административных функций управления | 5 |

Практика применения психологических средств и методов защиты информации в сфере деятельностно - административных функций управления

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**

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

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **10**

Проходной балл: **5**

| Показатели оценивания | Баллы |
|--|--------------|
| Разработка профилактических и коррекционных мероприятий с целью минимизации угроз со стороны человеческого фактора в сфере деятельностно-административных функций управления | 5 |
| диагностика угроз со стороны человеческого фактора в сфере деятельностно-административных функций управления | 5 |

Психологические средства и методы защиты информации в сфере организационных коммуникаций

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**

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

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **10**

Проходной балл: **5**

| Показатели оценивания | Баллы |
|---|--------------|
| Разработка профилактических и коррекционных мероприятий с целью минимизации угроз со стороны человеческого фактора в сфере организационных коммуникаций | 5 |
| Диагностика угроз со стороны человеческого фактора в сфере организационных коммуникаций | 5 |

Психологические средства и методы защиты информации в мотивационной сфере персонала и системе стимулирования организации

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**

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

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **5**

Проходной балл: **2.5**

| Показатели оценивания | Баллы |
|--|--------------|
| владеет знаниями групп риска в сфере трудовой мотивации, типов неконструктивной мотивации | 2 |
| владеет знаниями способов и приемов коррекции негативных явлений и угроз в мотивационной сфере сотрудников | 2 |
| владеет знаниями методов стимулирования персонала, способствующих поддержанию информационной безопасности | 1 |

Практика применения психологических средств и методов защиты информации в мотивационной сфере персонала и системе стимулирования организации

Продолжительность проведения мероприятия промежуточной аттестации: **6 часа**

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

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **10**

Проходной балл: **5**

| Показатели оценивания | Баллы |
|---|--------------|
| Разработка профилактических и коррекционных мероприятий с целью снижения угроз в сфере трудовой мотивации сотрудников | 5 |
| Диагностика угроз в сфере трудовой мотивации сотрудников. | 5 |

Профилактика и коррекция негативных социально - психологических явлений в системе информационной безопасности организации

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**

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

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **35**

Проходной балл: **15**

| Показатели оценивания | Баллы |
|---|--------------|
| Применение психологических средств и методов защиты информации в мотивационной сфере персонала и системе стимулирования организации | 10 |
| Применение психологических средств и методов защиты информации в сфере организационной культуры | 10 |
| Применение психологических средств и методов защиты информации в сфере деятельностно-административных функций управления | 8 |
| Психологические средства и методы защиты информации в сфере организационных коммуникаций | 7 |

Вид мероприятия промежуточной аттестации : Экзамен

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 48 до 60

«неудовлетворительно» / «незачтено» менее 48 балла

| Компетенция (индикатор) | Мероприятие текущего контроля | Контролируемые элементы результатов обучения |
|------------------------------------|--|---|
|------------------------------------|--|---|

| Компетенция (индикатор) | Мероприятие текущего контроля | Контролируемые элементы результатов обучения |
|---|--|---|
| <p>ПК.8 Способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем, а также положений, инструкций и других организационно-распорядительных документов</p> <p>ПК.10 Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах</p> <p>ПК.17 Способность разрабатывать планы работы первичных подразделений</p> | <p>Психологические средства и методы защиты информации в сфере групповой динамики организации.</p> <p>Письменное контрольное мероприятие</p> | <p>Письменная контрольная работа</p> |
| <p>ПК.8 Способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем, а также положений, инструкций и других организационно-распорядительных документов</p> <p>ПК.17 Способность разрабатывать планы работы первичных подразделений</p> | <p>Практика применения психологических средств и методов защиты информации в сфере групповой динамики организации</p> <p>Письменное контрольное мероприятие</p> | <p>Письменная лабораторная работа</p> |

| Компетенция (индикатор) | Мероприятие текущего контроля | Контролируемые элементы результатов обучения |
|---|--|---|
| ПК.17 Способность разрабатывать планы работы первичных подразделений | Психологические средства и методы защиты информации в сфере конфликтного взаимодействия сотрудников организации Письменное контрольное мероприятие | Письменная контрольная работа |
| ПК.7 Способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований | Практика применения психологических средств и методов защиты информации в сфере конфликтного взаимодействия сотрудников организации Письменное контрольное мероприятие | Письменная лабораторная работа |
| ПК.8 Способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем, а также положений, инструкций и других организационно-распорядительных документов ПК.17 Способность разрабатывать планы работы первичных подразделений | Психологические средства и методы защиты информации в сфере кадровой политики организации Письменное контрольное мероприятие | Письменная контрольная работа |

| Компетенция (индикатор) | Мероприятие текущего контроля | Контролируемые элементы результатов обучения |
|--|---|---|
| <p>ПК.8 Способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем, а также положений, инструкций и других организационно-распорядительных документов</p> <p>ПК.10 Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах</p> | <p>Практика применения психологических средств и методов защиты информации в сфере кадровой политики организации</p> <p>Письменное контрольное мероприятие</p> | <p>Письменная лабораторная работа</p> |

| Компетенция (индикатор) | Мероприятие текущего контроля | Контролируемые элементы результатов обучения |
|---|---|---|
| <p>ПК.5 Способность осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций</p> <p>ПК.7 Способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований</p> <p>ПК.8 Способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем, а также положений, инструкций и других организационно-распорядительных документов</p> <p>ПК.10 Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах</p> <p>ПК.17 Способность разрабатывать планы работы первичных подразделений</p> | <p>Организация системы информационной безопасности организации</p> <p>Итоговое контрольное мероприятие</p> | <p>Письменная контрольная работа</p> |

Спецификация мероприятий текущего контроля

Психологические средства и методы защиты информации в сфере групповой динамики организации.

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**

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

Максимальный балл, выставаемый за мероприятие промежуточной аттестации: **20**

Проходной балл: **9**

| Показатели оценивания | Баллы |
|---|--------------|
| Знание угроз в сфере ролевой структуры трудового коллектива | 10 |
| Знание угроз в сфере групповой динамики: групповых процессов, состояний, эффектов | 10 |

Практика применения психологических средств и методов защиты информации в сфере групповой динамики организации

Продолжительность проведения мероприятия промежуточной аттестации: **8 часа**

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

Максимальный балл, выставаемый за мероприятие промежуточной аттестации: **10**

Проходной балл: **5**

| Показатели оценивания | Баллы |
|---|--------------|
| Разработка профилактических и коррекционных мероприятий с целью минимизации угроз со стороны человеческого фактора в сфере групповой динамики | 5 |
| Диагностика угроз со стороны человеческого фактора в сфере групповой динамики организации | 5 |

Психологические средства и методы защиты информации в сфере конфликтного взаимодействия сотрудников организации

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**

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

Максимальный балл, выставаемый за мероприятие промежуточной аттестации: **10**

Проходной балл: **5**

| Показатели оценивания | Баллы |
|---|--------------|
| Знание технологий урегулирования конфликтов | 3 |
| Знание угроз со стороны человеческого фактора в сфере конфликтного взаимодействия | 3 |
| Знание типологии организационных конфликтов | 2 |
| Знание особенностей восприятия в конфликте | 2 |

Практика применения психологических средств и методов защиты информации в сфере конфликтного взаимодействия сотрудников организации

Продолжительность проведения мероприятия промежуточной аттестации: **8 часа**

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

Максимальный балл, выставаемый за мероприятие промежуточной аттестации: **10**

Проходной балл: **5**

| Показатели оценивания | Баллы |
|---|-------|
| Разработка мер по профилактике и коррекции угроз со стороны человеческого фактора в сфере конфликтного взаимодействия | 5 |
| Диагностика конфликтного взаимодействия в трудовом коллективе | 5 |

Психологические средства и методы защиты информации в сфере кадровой политики организации

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**

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

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **10**

Проходной балл: **5**

| Показатели оценивания | Баллы |
|---|-------|
| Знание угроз в сфере кадровой политики со стороны человеческого фактора | 5 |
| Знание типов кадровой политики | 5 |

Практика применения психологических средств и методов защиты информации в сфере кадровой политики организации

Продолжительность проведения мероприятия промежуточной аттестации: **6 часа**

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

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **10**

Проходной балл: **5**

| Показатели оценивания | Баллы |
|--|-------|
| Разработка рекомендаций с целью профилактики и коррекции угроз в сфере кадровой политики | 5 |
| Диагностика угроз в сфере кадровой политики. | 5 |

Организация системы информационной безопасности организации

Продолжительность проведения мероприятия промежуточной аттестации: **6 часа**

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

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

Проходной балл: **14**

| Показатели оценивания | Баллы |
|---|-------|
| Практика применения психологических средств и методов защиты информации в сфере групповой динамики организации | 10 |
| Практика применения психологических средств и методов защиты информации в сфере кадровой политики организации | 10 |
| Практика применения психологических средств и методов защиты информации в сфере конфликтного взаимодействия сотрудников организации | 10 |