Государственное бюджетное образовательное учреждение высшего образования Московской области

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ "ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А.ЛЕОНОВА"

Подписано цифровой подписью: ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ "ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А.ЛЕОНОВА"

«УТВЕРЖДАЮ»
Проректор по учебно-методической работе
И.В. Бабина
«12» апреля 2022 г.

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б.1.В.ДВ.04.01 «ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ ПЕРСОНАЛА ПРЕДПРИЯТИЯ»

Направление подготовки: 10.03.01 Информационная безопасность
Профиль: Безопасность телекоммуникационных систем (в аэрокосмической сфере)
Уровень высшего образования: бакалавр
Форма обучения: очная

Королев
2022

Рабочая программа является составной частью основной профессиональной образовательной программы и проходит рецензирование со стороны работодателей в составе основной профессиональной образовательной программы. Рабочая программа актуализируется и корректируется ежегодно.

Автор: Соляной В.Н. Рабочая программа дисциплины: «Информационно-психологическая безопасность персонала предприятия». – Королев МО: «Технологический университет», 2022.

Рецензент: **Сухотерин А.И.**

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки бакалавров 10.03.01 «Информационная безопасность» и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 12.04.2022 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	к.в.н., доцент Соляной В.Н.			
Год утверждения (переутверждения)	2022	2023	2024	2025
Номер и дата протокола заседания кафедры	№8 от 17.03.2022			

Рабочая программа согласована:

Руководитель ОПОП ВО к.т.н., доцент Вихров А.П.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2022	2023	2024	2025
Номер и дата протокола заседания УМС	№4 от 12.04.2022			

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОПОП ВО

Целями изучения дисциплины является:

1. Обучение студентов принципам и средствам обеспечения информационной безопасности личности (сотрудников), коллективов (организационных структур предприятий) и в целом общества (предприятий);
2. Получение студентами фундаментальных основ по формированию научного мировоззрения, развитию системного мышления и интеграции полученных ранее знаний по обеспечению информационной безопасности.

В процессе обучения студент приобретает и совершенствует следующие компетенции.

ПК-2. Способность принимать участие в проведении экспериментальных исследований системы защиты информации

ПК-3. Способность осуществлять управление с разработкой организационно-распорядительных документов и реализацию организационных мер по ЗИ в АС

Основными **задачами** дисциплины являются:

- дать основные знания, умения и навыки по вопросам обеспечения информационной безопасности личности (сотрудника), коллектива сотрудников (отделов, служб) и, в целом, всего коллектива предприятия как общества.

Показатель освоения компетенции отражают следующие индикаторы:

Необходимые знания:
- руководящие и методические документы принципы организации по проведению экспериментальной деятельности в области ЗИ;
- основные нормативно-правовые акты, методы управления деятельностью, угрозы ИБ и нарушители систем безопасности информации;

Необходимые умения:
- применять действующую нормативную базу выбирать целесообразные потребные средства и определять структуру системы ЗИ в ходе проведения экспериментов;
- оценивать информационные риски разрабатывать предложения по совершенствованию СУ (ИБ) и применять средства контроля эффективности ЗИ;

Трудовые действия:
- разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;

- анализировать воздействие на защищаемую систему информации, оценивать последствия и вырабатывать предложения по ее совершенствованию;

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Информационно-психологическая безопасность персонала предприятия» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОПК-1,6,7,8,9,13; УК-5,6,9.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Организация системы обеспечения информационной безопасности (служба ИБ)», «Лицензирование и сертификация в области защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

3. Объем дисциплины (модуля) и виды учебной работы

Общая трудоемкость дисциплины для студентов очной формы составляет **3** зачетных единицы, **108** часов.

Таблица1

Виды занятий	Всего часов	Семестр 6	Семестр …	Семестр 7	Семестр
Общая трудоемкость	**108**	**108**		**108**	
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	**48**	**48**			
Лекции (Л)	**16**	**16**			
Практические занятия (ПЗ)	**16**	**16**			
Лабораторные работы (ЛР)	**16**	**16**			
Практическая подготовка	-	-			
Самостоятельная работа	**50**	**50**			
Курсовые работы (проекты)	-	-			
Расчетно-графические работы	-	-			
Контрольная работа, домашнее задание	+	+			
Текущий контроль знаний (7 - 8, 15 - 16 недели)	**Т1, Т2**	**Т1, Т2**			
Вид итогового контроля	**Зачёт с оценкой**	**Зачёт с оценкой**			

4. Содержание дисциплины

4.1.Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. Очное	Практические занятия, Час Очное	Лабораторные занятия, Час Очное	Интерактивные Часы Очное	Код компетенций
Тема 1. Основы информационно-психологической безопасности	**3**	**3**	**3**	**Нет**	**ПК-2**
Тема 2. Человек и коллектив как субъекты информационно-психологических воздействий	**3**	**3**	**3**	**Нет**	**ПК-2**
Тема 3. Информационно-психологическое оружие: понятие, классификация и возможности	**3**	**3**	**3**	**Нет**	**ПК-2**
Тема 4. Обеспечение информационно-психологической безопасности личности	**3**	**3**	**3**	**Нет**	**ПК-3**
Тема 5. Информационно-психологическая безопасность кол-	**4**	**4**	**4**	**Нет**	**ПК-3**

лектива (групп) и коммуникативных процессов					
Итого:	**16**	**16**	**16**	**Нет**	

4.2. Содержание тем дисциплины

Раздел №1. Базовые положения информационно-психологической безопасности

Тема 1. Основы информационно-психологической безопасности

Информационно-психологическая безопасность как предмет научного анализа в информационной безопасности.

Основной понятийный аппарат дисциплины: информация, информационные обмены и информационные воздействия; специфические формы информационно-психологических воздействий: реклама, манипулирование, программирование (зомбирование), пропаганда, «промывание мозгов» и информационное оружие.

Информационные войны в структуре современной цивилизации: логика информационно-психологической войны – формирование нового поведения путем формирования новой картины мира; цель войны - воздействие на системы знаний и представлений. Особенности ведения информационно-психологических войн в современных условиях.

Тема 2. Человек и коллектив как субъекты информационно-психологических воздействий

Основы коммуникативной психологии: суть коммуникативных процессов и место человека в них; анализ концепций психологии массовой коммуникации.

Возможности человека по восприятию информации: модели обработки информации органами зрения, слуха, обоняния и вкуса. Формы познания информации человеком.

Психика человека. Сознание как высшая управляющая подсистема человека. Структура сознания, информационная защищенность и уязвимость.

Воздействие информации на память человека. Процесс внушающего воздействия на человека: процесс внушения; эффекты внушения и восприятия; механизмы внушающего воздействия.

Информативные признаки человека и общества и их классификация. Информативные каналы передачи признаков физиологического состояния человека. Признаки психологического состояния человека: национально-психологические признаки; индивидуально-личностные признаки и групповые информативные признаки.

Тема 3. Информационно-психологическое оружие: понятие, классификация и возможности

Определение понятия информационно-психологическое оружие. Объекты воздействия информационно-психологического оружия. Модель информационно-психологического воздействия на психику человека.

Общая классификация информационно-психологического оружия.

MASS-MEDIA- оружие (оружие массовой информации): устное вещание; радио и телевидение; кино, видеофильмы, аудиоматериалы; печатные и изобразительные средства;

компьютерные телекоммуникационные сети; предметы повседневного спроса с надписями.

Виртуальное информационно-психологическое оружие: виртуальные игрушки; виртуальные комплексы; виртуальные системы; виртуальные комплексы сопряжения с отрытыми телекоммуникационными сетями (в том числе глобальными); виртуальные города.

Энергоинформационное психологическое оружие: СВЧ-генераторы; ультра звуковые генераторы; генераторы инфразвука; источники когерентного света; источники некогерентного света.

Психотронно-информационное оружие: психотронные генераторы узконаправленного действия; ретрансляторы энергии космоса; многополюсные генераторы; спи-норные (торсионные) или ПИД- генераторы.

Психотропно-информационное оружие: нейролептики; транквилизаторы, антидепрессанты; псих-стимуляторы; психотомиметические средства.

Биоэнергоинформационное оружие: воздействие экстрасенсов (экстра-

сенсорика); гипнотическое воздействие (гипноз).

Информационно-генетическое и соматропно-психоинформационное оружие, лингвистическое и нейролингвистическое (программное) оружие. Электронные (виртуальные) деньги. Флэш-моб (внезапная толпа).

Раздел №2. Организация информационно-психологической безопасности на предприятии

Тема 4. Обеспечение информационно-психологической безопасности личности

Возможности человека и информационно-психологическая защита личности (сотрудника) и коллектива предприятия. Психологическая защита личности: определение понятия. Объект и предмет информационно-психологической защиты.

Базовые виды (формы) психологических защит: : бегство, прятание (уход в укрытие), замирание (маскировка), нападение (уничтожение, изгнание) и контроль (управление).

Формы защиты личности с соответствующим изменением их содержания: уход, изгнание (вытеснение), блокирование (блокировка, преграда, ограждение), управление (манипулирование), затаивание (замирание, маскировка), игнорирование.

Система психологической защиты личности: три основных уровня организации психологической защиты человека и, соответственно, три основных направления ее формирования и функционирования: социальный (в масштабах общества в целом); социально-групповой (в рамках различных социальных групп и разнообразных форм социальных организаций); индивидуально-личностный.

Тема 5. Информационно-психологическая безопасность коллектива (групп) и коммуникативных процессов

Понятие о социально-психологическом климате (безопасности) коллектива.

Группы защитных мер по обеспечению информационно-психологической безопасности коллектива: определяемые внутренней и внешней информационной средой.

Характеристика защитных мер по информационно-психологической безопасности, определяемых внутренней информационной средой (организационная самостоятельность и реализуемые меры): регулирование и ограничение информационных потоков(негативных воздействий); организация информационных потоков (инициирование распространения определенной положительной информации).

Характеристика защитных мер по информационно-психологической безопасности, определяемых изменением механизмов и способов взаимодействия человека/коллектива с внешней информационной средой.

5. Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине.

«Методические указания для самостоятельной работы обучающихся по освоению дисциплины» представлены в Приложении 2.

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине.

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине «информационно-психологическая безопасность персонала предприятий» приведена в Приложении 1.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1.Информационно-психологическая безопасность : учебно-методическое пособие / составитель С. Ю. Махов. — Орел : МАБИВ, 2020. — 135 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176395 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

2.Психологическая безопасность : учебно-методическое пособие / составитель С. Ю. Махов. — Орел : МАБИВ, 2020. — 170 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176396 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

3.Высочина, Н. Л. Психологическое обеспечение подготовки спортсменов в олимпийском спорте : монография / Н. Л. Высочина. — Москва : Спорт-Человек, 2021. — 304 с. — ISBN 978-5-907225-44-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/165156 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Интернет-ресурсы:

1. http://eup.ru/catalog/all-all.asp – научно-образовательный портал.
2. http://informika.ru/ – образовательный портал
3. www.wikIsec.ru - Энциклопедия информационной безопасности. – Публикации, статьи.
4. **www.biblioclub.ru** - Универсальная библиотека онлайн
5. **www.rucont.ru** - ЭБС «Руконт».
6. http://www.academy.it.ru/ – академия АЙТИ.
7. http://www.minfin.ru - Официальный сайт Министерства финансов Российской Федерации
8. http://www.gov.ru/ - Официальный сервер органов государственной власти Российской Федерации.
9. http://www.fsb.ru/ - Официальный сайт Федеральной Службы Безопасности
10. http://www.fstec.ru/ - Официальный сайт Федеральной Службы по Техническому Экспортному Контролю

9. Методические указания для обучающихся, по освоению дисциплины

Методические указания для обучающихся, по освоению дисциплины приведены в Приложении 2 к настоящей рабочей программе.

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

Перечень программного обеспечения: MSOffice, PowerPoint.

Информационные справочные системы:

Ресурсы информационно-образовательной среды МГОТУ:
Рабочая программа и методическое обеспечение по курсу: «Информационно-психологическая безопасность персонала предприятия».

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

Лекционные занятия:

- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций / слайдов на темы:

Практические занятия:

- компьютерный класс с проектором для интерактивного обучения и проведения лекций в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже WindowsXP; офисные программы MSOffice 7;
- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

Приложение 1

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ ПЕРСОНАЛА ПРЕДПРИЯТИЯ

Направление подготовки: 10.03.01 Информационная безопасность
Профиль: Безопасность телекоммуникационных систем (в аэрокосмической сфере)
Уровень высшего образования: бакалавр
Форма обучения: очная

Королев
2022

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

№ п/п	Индекс компетенции	Содержание компетенции	Раздел дисциплины, обеспечивающий формирование компетенции	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает:		
				Трудовые действия	Необходимые умения	Необходимые знания
1.	ПК-2	Способность принимать участие в проведении экспериментальных исследований системы защиты информации	Тема:1,2,3,4,5	- разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;	- применять действующую нормативную базу выбирать целесообразные потребные средства и определять структуру системы ЗИ в ходе проведения экспериментов;	- руководящие и методические документы принципы организации по проведению экспериментальной деятельности в области ЗИ;
2.	ПК-3	Способность осуществлять управление с разработкой организационно-распорядительных документов и реализацию организационных мер по ЗИ в АС	Тема:1,2,3,4,5	- анализировать воздействие на защищаемую систему информации, оценивать последствия и вырабатывать предложения по ее со-	- оценивать информационные риски разрабатывать предложения по совершенствованию СУ (ИБ) и применять средства контроля эффективн	- основные нормативно-правовые акты, методы управления деятельностью, угрозы ИБ и нарушители систем безопасности информации;

				вершен-ствованию	ости ЗИ;	

2.Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	Инструмент, оценивающий сформированность компетенции	Этапы и показатель оценивания компетенции	Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания
ПК-2,3	Доклад	А) полностью сформирована (компетенция освоена на высоком уровне) – 5 баллов Б) частично сформирована: • компетенция освоена на продвинутом уровне – 4 балла; • компетенция освоена на базовом уровне – 3 балла; В) не сформирована (компетенция не сформирована) – 2 и менее баллов	Проводится в письменной и/или устной форме. Критерии оценки: 1. Соответствие содержания доклада заявленной тематике (1 балл). 2. Качество источников и их количество при подготовке работы (1 балл). 3. Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4. Качество самой представленной работы (1 балл). 5. Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов.
ПК-2,3	Выполнение контрольной работы	А) полностью сформирована (компетенция освоена на высоком уровне) – 5 баллов Б) частично сформирована: • компетенция освоена на продвинутом уровне – 4 балла; • компетенция освоена на	При определении сформированности компетенций критериями оценивания выступают методические рекомендации, разработанные по дисциплине для данного вида

		базовом уровне – 3 балла; В) не сформирована (компетенция не сформирована) – 2 и менее баллов	

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерная тематика докладов в форме презентации:

1. Объект обеспечения информационно-психологической безопасности личности – индивидуальное сознание и подсознание.

2. Предмет обеспечения информационно-психологической безопасности личности - способность человека адекватно принимать решения в условиях негативных информационных воздействий.

3. Источники и информационные угрозы индивидуальному сознанию личности.

4. Объект обеспечения информационно-психологической безопасности коллектива – групповое сознание.

5. Предмет обеспечения информационно-психологической безопасности коллектива - способность коллектива достигать поставленные цели в условиях негативных информационных воздействий.

6. Источники и информационные угрозы групповому сознанию коллективу.

7. Объект обеспечения информационно-психологической безопасности общества – массовое сознание.

8. Предмет обеспечения информационно-психологической безопасности общества - способность общества поддерживать и развивать установившиеся общественные отношения граждан и коллективов в условиях негативных информационных воздействий.

9. Источники и информационные угрозы массовому сознанию общества.

10. Система обеспечения информационно-психологической безопасности на предприятии.

11. Нормативно-правовая составляющая системы обеспечения информационно-психологической безопасности на предприятии.

12. Организационная составляющая система обеспечения информационно-психологической безопасности на предприятии.

13. Технологическая составляющая системы обеспечения информационно-психологической безопасности на предприятии.

14. Кадровая составляющая системы обеспечения информационно-психологической безопасности на предприятии.

15. Основные проблемы обеспечения информационно-психологической безопасности.

16. Разработка основ государственной политики обеспечения информационно-психологической безопасности.

17. Развитие системы информационно-аналитической деятельности на предприятии как направление совершенствования информационно-психологической безопасности.

18. Оценка рисов при обеспечении информационно-психологической безопасности личности.

19. Оценка рисов при обеспечении информационно-психологической безопасности коллективов.

20. Технология ведения переговоров-информационно-психологический аспект.

21. Технологии информационно-психологического влияния на личность и защита его от информационных негативных воздействий.

22. Технологии информационно-психологического влияния на коллектив и защита его от информационных негативных воздействий.

23. Безопасное социально-информационное воздействие в современном обществе.

24.Современные Интернет-технологии в области обеспечения информационно-психологической безопасности личности.

25. Современные Интернет-технологии в области обеспечения информационно-психологической безопасности коллективов.

26. Обеспечение энергоинформационной психологической безопасности в современных условиях.

27. Социальная инженерия и информационно-психологическая безопасность.

Примерная тематика заданий на контрольную работу:

1. Законодательство России об информационно-психологической безопасности.

2. Принципы обеспечения информационно-психологической безопасности

3. Угрозы негативных информационно-психологических воздействий

4. Государственная система обеспечения информационно-психологической безопасности

5. Функции государственной системы обеспечения информационно-психологической безопасности

6. Органы государственной системы обеспечения информационно-психологической безопасности

7. Организации обеспечения информационно-психологической безопасности

8. Лицензирование в области обеспечения информационно-психологической безопасности

9. Сертификация средств и методов обеспечения информационно-психологической безопасности

10. Экспертиза в целях выявления негативных информационно-психологических воздействий

11. Контроль за обеспечением информационно-психологической безопасности

12. Применения специальных средств и методов информационно-психологического воздействия

13. Международное сотрудничество в области обеспечения информационно-психологической безопасности

14. Ответственность за нарушение официальных положений (требований) по обеспечению информационно-психологической безопасности

15. Финансирование деятельности, связанной с обеспечением информационно-психологической безопасности

16. Новейшие современные средства и методы информационно-психологического воздействия на системы управления живых организмов.

17. Современные средства и методы информационно-психологического воздействия на сознание личности.

18. Современные средства и методы информационно-психологического воздействия на подсознание личности.

19. Современные средства и методы информационно-психологического воздействия на коллективы людей.

20. Проблема обеспечения информационно-психологической безопасности для России.

21. Проблема обеспечения информационно-психологической безопасности для мирового сообщества

22. Международное право, направленное на защиту психики человека от негативных информационно-психологических воздействий.

23. Государственная политика РФ по обеспечению информационно-психологической безопасности.

24. Организация обучения людей методам защиты от негативных информационно-психологических воздействий на их психику.

25. Разработка и использование специальных стандартов в области обеспечения информационно-психологической безопасности.

26. Государственный и гражданский контроль бесконтрольного применения специальных средств и методов негативного информационно-психологического воздействия.

27. Принцип государственной монополии на использование специальных средств и методов воздействия на психику людей.

28. Координация деятельности органов, входящих в государственную систему обеспечения информационно-психологической безопасности.

29. Разработка концепции по обеспечения информационно-психологической безопасности РФ.

30. Разработка концепции по обеспечения информационно-психологической безопасности предприятия.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Формой контроля знаний по дисциплине «Информационно-психологическая безопасность персонала предприятия» являются две текущие аттестации в виде тестов и итоговая аттестация в виде зачёта с оценкой.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
Проводится в сроки, установленные графиком образовательного процесса	тестирование	ПК-2,3	20 вопросов	Компьютерное тестирование ; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.***

Проводится в сроки, установленные графиком образовательного процесса	тестирование	ПК-2,3	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.***
Проводится в сроки, установленные графиком образователь	Зачёт с оценкой	ПК-2,3	3 вопроса	Зачёт с оценкой проводится в письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	Результаты предоставляются в день проведения зачета с оценкой	Критерии оценки: «**Отлично**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических

ного процесса						занятиях; • знание основных научных теорий, изучаемых предметов; • ответ на вопросы билета. «**Хорошо**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответы на вопросы билета • неправильно решено практическое задание «У**довлетвори-тельно**»: • демонстрирует частичные знания по темам дисциплин

						; • незнание неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; «**Неудовлетворительно**»: • демонстрирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; • не отвечает на

						вопросы.

4.1. Типовые вопросы, выносимые на тестирование

Тесты используются в режиме промежуточного контроля. По форме заданий выбраны закрытые тесты (с выборочным ответом). Каждому вопросу соответствует один вариант ответа.

1. С какой тайной связывают банковскую тайну?

(!) Коммерческая тайна

(?) Государственная тайна

(?) Служебная тайна

(?) Тайна следствия и судопроизводства

2. Какие операции не могут осуществляться при банковских отношениях?

(?) Привлечение во вклады денежных средств физических и юридических лиц

(?) Открытие и ведение счетов физических и юридических лиц

(?) Размещение указанных средств от своего имени и за свой счет на условиях возврата

(!) Размещение указанных средств от своего имени и за свой счет

3. Какова величина суммы застрахованного банковского вклада?

(!) 1 млн. 400 тыс. руб.

(?) 800 тыс. руб.

(?) 100 тыс. руб.

(?) 150 тыс. руб.

4. Основной законодательный акт, в котором определена Банковская Тайна?

(?) Конституция РФ

(?) ФЗ. № 149 «Об информации, информационных технологиях и защите информации»

(!)ФЗ. № 395-1 «О Банках и Банковской деятельности»

(?) Доктрина ИБ

5. Кредитная организация не вправе осуществлять…?

(!) Лизинговые операции

(!) Оказание консультаций и информационных услуг

(!) Осуществление операций с драгоценными металлами и камнями в соответствии с законами

(?) Осуществление операций с драгоценными металлами и камнями

6. В соответствии, с каким законом сотрудник подписывает документ о неразглашении?

(?) Конституция РФ

(!) ФЗ. №86 «О ЦБ РФ»

(?) УК РФ

(?) ФЗ «О коммерческой тайне»

7. В соответствии, с каким законом обеспечивается сохранность ПД при аудиторских проверках?

(?) ФЗ. № 149 «Об информации, информационных технологиях и защите информации»

(?) ФЗ. №86 «О ЦБ РФ»

(?) ФЗ. № 395-1 «О Банках и Банковской деятельности»

(!) ФЗ. №107 «Об аудиторской деятельности»

8. Кто занимается созданием центральной базы кредитных историй?

(?) Вкладчик

(!) Бюро кредитных историй

(?) Специалист по ИБ

(?) Банк

9. Кому не может быть предоставлен кредитный отчет?

(?) Пользователь кредитной истории

(?) Субъекту кредитных историй

(?) В суд

(!) Родственникам

10. Обязательно ли попадет кредитная история в центральное бюро кредитных историй?

(!) Обязательно

(?) По желанию

(?) Не попадет

(?) Попадет через 5 лет

11. В соответствии, с каким законом осуществляется страхование счетов?

(?) ФЗ. №86 «О ЦБ РФ»

(?) ФЗ. № 395-1 «О Банках и Банковской деятельности»

(?) Конституцией РФ

(!) ФЗ. №177 «О страховых вкладах физических лиц в банковских организациях»

12. Чем регламентируется работа бюро кредитных историй?

(!) Законом о кредитных историях

(?) Конституцией РФ

(?) Уголовным кодексом

(?) Банком

13. Кредитная история хранится в течении?

(!) 15 лет с последнего изменения

(?) 16 лет с последнего изменения

(?) 10 лет с последнего изменения

(?) 5 лет с последнего изменения

14. Что не входит в кредитную историю?

(!) Сведения о месте работы

(?) ФИО

(?) Данные паспорта

(?) Индивидуальный номер налогоплательщика

15. Правом на сохранение БТ не обладает?

(!) Государство

(?) Доверитель

(?) Клиент

(?) Корреспондент

16.Согласно закону РФ «Об авторском праве» автор это:

(!) физическое лицо, творческим трудом которого создано произведение;

(?) юридическое лицо, творческим трудом которого создано произведение;

(?) физическое лицо, физическим трудом которого создано произведение;

(?) юридическое лицо, умственным трудом которого создано произведение.

17. Авторское право это:

(!) институт гражданского права, регулирующий отношения, связанные с созданием и использованием (изданием, исполнением, показом и т. д.) результатов творческой деятельности людей;

(?) институт гражданского права, регулирующий отношения, связанные с созданием и использованием (изданием, исполнением, показом и т. д.) периодических произведений;

(?) институт гражданского права, регулирующий отношения, связанные с разработкой нормативно правовой базы предприятий;

(?) институт уголовного права, регулирующий отношения, связанные с совершением преступных деяний.

18. Что из перечисленного относится к смежным правам:

(!) гражданские правоотношения тесно связанные с авторским правом, возникающие в ходе реализации исполнительных прав и прочих прав;

(?) гражданские правоотношения тесно связанные с авторским правом, возникающие в случае утери автором оригинала произведения;

(?) гражданские правоотношения тесно связанные с авторским правом, возникающие в ходе продажи авторских прав;

(?) юридические правоотношения не связанные с авторским правом.

19. Что не является объектом авторского права:

(?) фольклор;

(!) литературные произведения;

(!) музыкальные произведения;

(!) скульптуры.

20. После смерти автора, авторское право защищается в течении:

(!) 70 лет;

(?) 25 лет;

(?) 10 лет;

(?) 100 лет.

21. К неделимому соавторству относится:

(!) случаи, когда произведение образует неразрывное целое;

(?) случаи, когда созданное в соавторстве произведение состоит из частей, имеющих самостоятельное значение;

(?) случаи, когда произведение состоит из взаимозаменяемых частей;

(?) случаи, когда деление произведения не рассмотрено в договоре соавторов.

22. Право на произведение, обнародованное под псевдонимом, действует в течении:

(!) 70 лет;

(?) 100 лет;

(?) 25 лет;

(?) 10 лет.

23. Правовому регулированию смежных прав посвящается:

(!) часть 4 гражданского кодекса РФ;

(?) ФЗ №101 «Об авторском праве и смежных правах»;

(?) Постановление правительства РФ №93 «О смежных правах»;

(?) Указ президента РФ №60 «Перечень смежных прав».

24. Право на отзыв это:

(!) право позволяющее автору отказаться от ранее принятого решения об обнародовании произведения;

(?) право позволяющее другому лицу делать отзыв на произведение;

(?) право на составление отзыва на собственное произведение;

(?) право позволяющее автору отказаться от ранее принятого решения о составлении отзыва.

25. Произведение считается обнародованным если:

(!) в течении 30 дней после опубликования за пределами РФ оно было опубликовано на территории РФ;

(?) в течении 40 дней после опубликования за пределами РФ оно было опубликовано на территории РФ;

(?) после 10 дней поле опубликования в РФ;

(?) сразу после опубликования в РФ.

26. К авторским правам не относятся:

(!) специальное право;

(?) исключительное право;

(?) личные не имущественные права;

(?) иные права.

27. К личным не имущественным правам не относится:

(!) право на продажу произведения;

(?) право на обнародование произведения;

(?) право на имя;

(?) право авторства.

28. К исключительному праву относятся:

(!) право распространения;

(!) право публичного показа;

(?) право на отзыв;

(?) право на имя.

29. К иным правам не относится:

(!) право на издание;

(?) право на отзыв;

(?) право следования;

(?) право доступа.

30. Авторское право действует на:

(!) обнародованное произведение;

(!) необнародованное произведение;

(?) чужое произведение;

(?) федеральный закон.

31. Определение коммерческой тайны в соответствии с ФЗ «О коммерческой тайне»:

(!) Информация, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;

(?) Информация, имеющая реальную или потенциальную ценность, в силу её неизвестности третьим лицам;

(?) Информация, которая может нанести ущерб, в случае её разглашения;

(?) Информация о деятельности коммерческой организации, которая может нанести непоправимый ущерб, в случае утечки.

32. Конфиденциальная составляющая коммерческой тайны:

(!) Конфиденциальная информация, отражающая следующие аспекты коммерческой деятельности: технические, экономические, организационные;

(?) Информация о коммерческой деятельности фирмы внутреннем и внешнем рынках;

(?) Информация об организационном порядке по работе с информацией конфиденциального характера;

(?) Персональные данные руководящего состава предприятия.

33. Интеллектуальная составляющая коммерческой тайны:

(!) Не обнародованные в официальном порядке результаты интеллектуальной деятельности: изобретения, полезные модели, промышленные образцы, оригинальные технологии, оригинальный набор информационных подходов;

(?) Обнародованные в официальном порядке результаты интеллектуальной деятельности: изобретения, полезные модели, промышленные образцы, оригинальные технологии, оригинальный набор информационных подходов;

(?) Документально зафиксированная информация об использовании и применении оригинальных технологий и подходов на предприятии;

(?) Часть коммерческой тайны, которая в явном виде не присутствует в перечне сведений, подразумевается.

34. Кем и когда утверждён, перечень сведений конфиденциального характера:

(!) Указ президента от 6 марта 1997 года №188;

(?) Постановление правительства от 5 декабря 2003 года № 89;

(?) Федеральный закон от 27 декабря 2002 года № 184-ФЗ;

(?) Федеральный закон от 28 декабря 2010 года № 390-ФЗ

35. Назовите документ, связанный с защитой информации, составляющей коммерческую тайну, посвящённый требованиям и рекомендациям по технической защите конфиденциальной информации

(!) «Специальные требования и рекомендации по защите конфиденциальной информации» решение президиума гостехкомиссии России № 7.2 от 2 марта 2001 года.

(?) Федеральный закон № 149 «Об информации, информационных технологиях и о защите информации»;

(?) Федеральный закон № 98 «О коммерческой тайне»;

(?) Гражданский кодекс РФ часть 4.

36. Какой нормативно - правовой акт регламентирует включение в договор с работодателем, условий о неразглашении охраняемой законом коммерческой тайны:

(!) Трудовой кодекс РФ;

(?) Федеральный закон «О коммерческой тайне»;

(?) Гражданский кодекс РФ;

(?) Уголовный кодекс РФ.

37. Каким документом определяются условия отнесения информации к сведениям, составляющим коммерческую тайну, обязанность соблюдения конфиденциальности такой информации, а так же ответственность за её разглашение:

(!) Федеральный закон № 149 «Об информации, информационных технологиях и о защите информации»;

(?) Гражданский кодекс РФ;

(?) Уголовный кодекс РФ;

(?) Федеральный закон № 98 «О коммерческой тайне».

38. Каким нормативно-правовым актом определяется защита элементов коммерческой тайны, которые рассматриваются как объекты интеллектуальной деятельности:

(!) Гражданский кодекс РФ от 18 декабря 2006 г. № 230-ФЗ часть 4. Глава 75 (право на секрет производства (ноу-хау));

(?) Федеральный закон «О коммерческой тайне»;

(?) Руководящий документ ФСТЭК «Специальные требования и рекомендации по защите конфиденциальной информации» (СТР-К)

(?) Уголовно-процессуальный кодекс РФ.

39. Какие требования предъявляются к лицу-обладателю информацией, составляющей коммерческую тайну:

(!) Оно владеет на законном основании; оно ограничивает доступ к информации, и установило режим коммерческой тайны в отношении этой информации;

(?) Оно является гражданином РФ; оно является законным держателем информации; оно обеспечивает защиту закрытой информации;

(?) Оно является юридическим лицом; оно установило режим конфиденциальной информации в отношении этой информации,

(?) Оно владеет информацией на законном основании; оно является гражданином РФ, проживающим на территории РФ не менее пяти лет; оно ограничило доступ к информации.

40. Признаки информации, обретённой незаконно:

(!) Получатель умышленно преодолевал меры по её охране; получатель знал, что получает информацию от лица, не имеющего право на её передачу получателю;

(?) Информация, так или иначе, имеет отношение к деловой активности конкретной фирмы;

(?) Информация, полученная из открытых источников;

(?) Плагиат.

41. Каким законом определяется порядок предоставление информации, составляющей коммерческую тайну:

(!) Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»

(?) Руководящий документ ФСТЭК «Специальные требования и рекомендации по защите конфиденциальной информации» (СТР-К)

(?) Федеральный закон № 149 « Об информации, информационных технологиях и о защите информации»;

(?) Федеральный закон № 98 «О коммерческой тайне».

42. Дать определение контрагента в соответствии с ФЗ № 98 «О коммерческой тайне»:

(!) Сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию;

(?) Сторона соглашения, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию;

(?) Обладатель информации;

(?) Лицо, которому стала известна информация, в силу исполнения им служебных обязанностей.

43. Общие меры обеспечения соблюдения конфиденциальности информации:

(!) Разработка перечня информации, ограничение и регламентирование доступа, разработка и регулирование правил по регулированию отношений, нанесение на документы грифа коммерческой тайны;

(?) Разработка и регулирование правил организации обращения с конфиденциальной информацией;

(?) Организация конфиденциального документооборота на предприятии;

(?) Заключение соглашения с сотрудниками по обработке конфиденциальной информации.

44. Каких правил должен придерживаться работник при обработке информации конфиденциального характера:

(!) Выполнять установленный режим защиты, не разглашать сведения, составляющие коммерческую тайну; после прекращения трудовых отношений, вернуть работодателю все документы, составляющие коммерческую тайну;

(?) Не разглашать сведения, составляющие коммерческую тайну; выполнять установленный режим защиты;

(?) Выполнять обязанности, согласно ФЗ № 149 «Об информации, информационных технологиях и о защите информации»;

(?) Выполнять требования инструкции по организации обработки конфиденциальной информации в организации.

45. Срок действия права на секрет производства, с грифом коммерческая тайна:

(!) Действует до тех пор, пока сохраняется конфиденциальность сведений, составляющих коммерческую тайну в соответствии с гражданским кодексом РФ «Исключительное право на секрет производства» ст. 1467;

(?) Право на секрет производства с грифом коммерческая тайна не имеет срока давности;

(?) Право на секрет производства с грифом коммерческая тайна составляет тридцать календарных дней, с момента присвоения грифа;

(?) Действует до тех пор, пока сохраняется конфиденциальность сведений, составляющих коммерческую тайну, согласно федеральному закону № 98;

Кто утвердил перечень сведений конфиденциального характера № 188:

(!)Президент.

(?)Премьер министр.

(?)ФСТЭК.

(?)ФСБ.

46. Что понимается под мошенничеством, согласно статьи №159 УК РФ

(!)Хищение имущества или приобретение права на чужое имущество путем злоупотребления доверием.

(?)Хищение имущества.

(?)Приобретение права на чужое имущество с помощью злоупотребления доверием.

(?)Получение имущества с помощью применения силы.

47. К правовым методам защиты информации доктрина относит:

(!)Разработка нормативно правовых актов, регламентирующих отношение в информационной сфере.

(?)Составление списка ответственных лиц.

(?)Указание по использованию физических средств ЗИ.

(?)Указание по использованию технических средств ЗИ.

48. Сколько видов конфиденциальной информации существует в соответствии с указом президента №188 1997 года?

(?)5.

(?)4.

(!)6.

(?)8.

49. Врачебная тайна, адвокатская тайна, нотариальная тайна, тайна переписки. К какому виду конфиденциальной информации относятся перечисленные тайны?

(?)Служебная тайна.

(?)Коммерческая тайна.

(?)Персональные данные.

(!)Профессиональная тайна.

50. Субъектами банковской тайны являются:

(!)Держатели.

(!)Кредитные организации.

(?)Вкладчики.

(?)Государство.

51. Определение организационно-розыскной деятельности

(!)Вид деятельности, осуществляющий по средствам ОРМ в целях защиты конституционных прав гражданина.

(?)Вид деятельности, направленный на безопасность общества, государства, личности.

(?)Вид деятельности, осуществляющийся по средства ОРМ в целях раскрытия инцидентов нарушения ИБ.

52. Какие сведения относятся к информации конфиденциального характера

(!)Сведения о возможных природных бедствиях.

(?)Информация, составляющая тайну следствия.

(?)Сведения, связь с профессиональной деятельностью.

(?)Сведения, связь с коммерческой деятельностью.

53. Информация, составляющая коммерческую тайну:

(?)Товарные знаки.
(?)Авторское право.
(?)Государственная тайна.
(!)Банковская тайна.

54. Чем охраняется информация, ограниченного доступа?

(!)Федеральными законами.
(?)Ведомственными приказами.
(?)Силовыми структурами (ведомствами).

55. За разглашение сведений конфиденциального характера наступает ответственность:

(?)Уголовная.
(?)Административная.
(?)Дисциплинарная.
(!)Все вышеперечисленные.

56. С правовой точки зрения защите подлежит:

(?)Любая закрытая информация.
(!)Информация, зафиксированная на материальном носителе.
(?)Любая коммерческая тайна.
(?)Всё вышеперечисленное.

4.2. Типовые вопросы, выносимые на зачёт с оценкой

1. Понятия, виды и формы «информационно-психологических воздействий» в сфере безопасности граждан и общества.
2. Информационно-психологическое оружие в современных условиях развития информационного общества.
3. Информационно-психологическая война в системе современных информационных войн.
4. Объект и субъект обеспечения информационно-психологической безопасности.
5. Принципы обеспечения информационно-психологической безопасности.
6. Основные направления обеспечения информационно-психологической безопасности фирмы.
7. Правовое регулирование обеспечения информационно-психологической безопасности граждан РФ.

8. Функции государственной системы обеспечения информационно-психологической безопасности в РФ.

9. Понятия «информационно-психологическая безопасность» в сфере безопасности предприятия.

10. Сущность информационно-психологической безопасности персонала в деятельности службы информационной безопасности предприятии.

11. Психика человека и его сознание как субъекты информационно-психологического воздействия (информационная защищенность и уязвимость).

12. Групповое и корпоративное сознание как субъекты информационно-психологического воздействия (информационная защищенность и уязвимость).

13. Психология массовой информационной коммуникации как субъекты информационно-психологического воздействия (информационная защищенность и уязвимость).

14. Признаки информационно-психологического состояния человека: национально-психологические признаки; индивидуально-личностные признаки и групповые информативные признаки.

15. Содержание и задачи по обеспечению информационно-психологической безопасности персонала и коллектива в системе безопасности предприятия.

16. Психика человека и его подсознание как субъекты информационно-психологич

17. Определение понятия информационно-психологическое оружие и его объекты воздействия.

18. Источники поступления угроз в системе информационно-психологической безопасности предприятия.

19. Модель информационно-психологического воздействия на психику человека.

20. Общая классификация информационно-психологического оружия.

21. Характеристика MASS-MEDIA- оружие (оружие массовой информации).

22. Характеристика виртуального информационно-психологического оружия.

23. Характеристика энергоинформационно-психологического оружия.

24. Психотронно-информационное и психотропно-информационное оружие.

25. Характеристика биоэнергоинформационного оружия.

26. Информационно-генетическое и соматропно-психоинформационное оружие.

27. Лингвистическое и нейролингвистическое (программное) оружие.

28. Информационно-психологическое оружие: электронные (виртуальные) деньги и «Флэш-моб» (внезапная толпа).

29. Информационно-психологическая защита человека и коллектива: определение, объект и предмет информационно-психологической защиты.

30. Основы организации информационно-психологической безопасности на предприятии.

31. Базовые виды (формы) информационно-психологической защиты.

32. Система (уровни) информационно-психологической защиты личности (персонала).

33. Характеристика социального (в масштабе общества в целом) уровня организации информационно-психологической защиты человека (персонала).

34. Характеристика социально-группового (в рамках различных социальных групп и разнообразных форм социальных организаций) уровня организации информационно-психологической защиты человека (персонала).

35. Характеристика индивидуально-личностного уровня организации информационно-психологической защиты человека (персонала).

36. Понятие о социально-психологическом климате (информационно-психологической безопасности) коллектива.

37. Общая характеристика групп защитных мер по обеспечению информационно-психологической безопасности коллектива (определяемые внутренней и внешней информационной средой).

38. Характеристика защитных мер по обеспечению информационно-психологической безопасности коллектива, определяемые внутренней информационной средой.

39. Характеристика защитных мер по обеспечению информационно-психологической безопасности коллектива, определяемые внешней информационной средой.

40. Особенности информационно-психологической безопасности коллективов (групп) в коммуникативных процессах.

41. Защитные меры по информационно-психологической безопасности, определяемые изменением механизмов и способов взаимодействия человека/коллектива с внешней информационной средой.

42. Средства и технологии обеспечения информационно-психологической безопасности персонала предприятия.

43. Средства и технологии обеспечения информационно-психологической безопасности коллективов на предприятии.

44. Критерии оценки эффективности обеспечения информационно-психологической безопасности персонала предприятия.

45. Планирование обеспечения информационно-психологической безопасности на предприятии.

46. Лицензирование в области обеспечения информационно-психологической безопасности.

47. Сертификация средств и методов обеспечения информационно-психологической безопасности.

48. Государственная экспертиза в целях выявления негативных информационно-психологических воздействий.

49. Организация контроля обеспечения информационно-психологической безопасности.

50. Международное сотрудничество в области обеспечения информационно-психологической безопасности.

**Итоговое начисление баллов по дисциплине осуществляется в соответствии с разработанной и внедренной балльно-рейтинговой системой контроля и оценивания уровня знаний и внеучебной созидательной активности обучающихся.*

Приложение 2

Методические указания для обучающихся по освоению дисциплины

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ ПЕРСОНАЛА ПРЕДПРИЯТИЯ

Направление подготовки: 10.03.01 Информационная безопасность
Профиль: Безопасность телекоммуникационных систем (в аэрокосмической сфере)
Уровень высшего образования: бакалавр
Форма обучения: очная

Королев
2022

1. Общие положения

Основными формами обучения студентов являются аудиторные занятия, включающие лекции и семинарские занятия.

Лекционные занятия проводятся в форме классической лекции. Лекционный материал в основном подготовлен в виде презентаций MS Power Point и предназначен для усвоения студентами теоретического материала. Ведение конспектов считается обязательным для более полного усвоения материала.

Семинарские занятия проводятся в форме обсуждения, закрепления и углубления учебного материала по отдельным вопросам изучаемых тем, изложенным ранее на лекционных занятиях, изучения структурных схем и основам работы отдельных должностных лиц службы информационной безопасности на типовом предприятии.

2. Указания по проведению практических занятий

Практическое занятие 1.
Вид практического занятия**:** ***подготовка доклада.***
Образовательные технологии: ***групповая дискуссия.***
Тема и содержание практического занятия:

Семинар 1. ***Основы информационно-психологической безопасности***
/3 час./

Учебные вопросы

1 занятие - 1час.

1. Основной понятийный аппарат области информационно-психологической безопасности личности и общества: информация, информационные обмены и информационные воздействия.
2. Особенности ведения информационно-психологических войн в современных условиях (понятии: информационная и информационно-психологические войны; информационное и информационно-психологическое оружие).
3. Специфические формы информационно-психологических воздействий: реклама, манипулирование, программирование (зомбирование), пропаганда,

«промывание мозгов».

2 занятие - 2час.

4. Понятие и содержание информационно-психологической безопасности в системе обеспечения информационной безопасности предприятия.
5. Цель и задачи информационно-психологической защиты сотрудников и производственных коллективов.
6. Основные направления обеспечения информационно-психологической безопасности на предприятии.

Продолжительность занятия – *3 ч.*

Практическое занятие 2.
Вид практического занятия**: *подготовка доклада.***
Образовательные технологии: ***групповая дискуссия.***
Тема и содержание практического занятия:

Семинар 2. ***Человек и коллектив как субъекты информационно-психологических воздействий***
/3 час./

Учебные вопросы

1 занятие - 1час.

1.Основы информационно-коммуникативных процессов человека и коллективов (общества).

2. Возможности человека по восприятию информации и модели обработки информации органами зрения, слуха, обоняния и вкуса.

3. Психика и сознание человека, их информационная защищенность и уязвимость.

2 занятие - 2час.

4. Процесс внушающего воздействия на человека: сущность внушения; эффекты внушения и восприятия; механизмы внушающего воздействия.

5. Информативные признаки человека и общества и их классификация.

6.Информативные каналы передачи признаков человека: физиологического состояния и психологического состояния

7. Национально-психологические, индивидуально-личностные и групповые информативные признаки.

Продолжительность занятия – *3 ч.*

Практическое занятие 3.
Вид практического занятия**: *подготовка доклада.***
Образовательные технологии: ***групповая дискуссия.***
Тема и содержание практического занятия:

Семинар 3. ***Информационно-психологическое оружие: понятие, классификация и возможности***

/3 час./

Учебные вопросы

1 занятие - 1час.

1.Определение понятия информационно-психологическое оружие и объекты их воздействия.

2. Модель информационно-психологического воздействия на психику человека.

3. Общая классификация информационно-психологического оружия.

2 занятие - 2час.

4.Характеристика MASS-MEDIA и виртуального информационно-психологического оружия.

5.Характеристика энергоинформационного психологического оружия.

6.Характеристика психотронно-информационного и психотропно-информационного оружия.

7.Характеристика информационно-генетического и соматропно-психоинформационного оружия.

8.Характеристика биоэнергоинформационное и информационно-генетическое оружия.

9. Характеристика биоэнергоинформационное и информационно-генетическое оружия.

Практическое занятие 4.
Вид практического занятия**: *подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***
Тема и содержание практического занятия:

Продолжительность занятия – *3 ч.*

Семинар 4. ***Обеспечение информационно-психологической безопасности личности***

/3 час./

Учебные вопросы

1 занятие - 2час.

1.Возможности человека и психологическая защита личности (сотрудника предприятия).

2. Базовые виды (формы) психологических защиты личности: бегство, прятание (уход в укрытие), замирание (маскировка), нападение (уничтожение, изгнание) и контроль (управление).

3.Формы защиты личности с соответствующим изменением их содержания: уход, изгнание (вытеснение), блокирование (блокировка, преграда, ограждение), управление (манипулирование), затаивание (замирание, маскировка), игнорирование.

2 занятие - 1час.

4.Система психологической защиты личности: три основных уровня организации психологической защиты человека.

5.Основные направления формирования и функционирования психологической защиты личности: социальное (в масштабах общества в целом); социально-групповое (в рамках различных социальных групп и разнообразных форм социальных организаций); индивидуально-личностное.

Продолжительность занятия – *3 ч.*

Практическое занятие 5.
Вид практического занятия**: *подготовка доклада.***
Образовательные технологии: ***групповая дискуссия.***
Тема и содержание практического занятия:

Семинар 5. ***Информационно-психологическая безопасность коллек-***

тива (групп) и коммуникативных процессов

/ 4час./

Учебные вопросы

1 занятие - 1час.

1.Понятие о социально-психологическом климате (безопасности) коллектива.

2.Группы защитных мер по обеспечению информационно-психологической безопасности коллектива: определяемые внутренней и внешней информационной средой.

2 занятие - 2час.

3.Сущность и состав типовых защитных мер по информационно-психологической безопасности коллектива, определяемые внутренней информационной средой предприятия (организационная самостоятельность и реализуемые меры).

4.Характеристика отдельных защитных мер по информационно-психологической безопасности коллектива (определяемые внутренней информационной средой): регулирование и ограничение негативных информационных потоков (воздействий); организация информационных потоков (инициирование распространения определенной положительной информации).

3 занятие - 1час.

5.Сущность и состав типовых защитных мер по информационно-психологической безопасности коллектива, определяемых изменением взаимодействия человека/коллектива с внешней информационной средой.

6. Характеристика отдельных защитных мер по информационно-психологической безопасности, определяемых изменением взаимодействия человека/коллектива с внешней информационной средой: видоизменение привлекаемых механизмов и использования новых способов (технологий).

Продолжительность занятия – *4 ч.*

3. Указания по проведению лабораторных работ

Цель проведения лабораторных работ – ознакомление студентов с комплексом показателей для оценки защищённости информационных объектов, систем и ознакомление с программной средой, используемой для моделирования процессов оптимизации применения систем физической защиты.

Задачи выполнения лабораторных работ:

- определение положения механизмов защиты, включение которых в иерархию системы физической защиты информационных объектов повышает уровень их защищённости;
- мониторинг защищённости охраняемых информационных объектов, базирующийся на решении оптимизационных задач на основе рейтинговых показателей, учитывающий разноплановые экспертные оценки, включая экономические;
- анализ существующих систем физической защиты предприятий на предмет определения эффективности их применения исходя из предполагаемых затрат на создание таких систем, их эксплуатацию и реализацию для предотвращения ущерба от выявленных и потенциальных угроз;
- формирование потенциальной структуры защищённых информационных систем и технологий, путём задания иерархии эшелонов и перечня механизмов защиты для нейтрализации требуемого поля угроз и предотвращённого ущерба;
- формирование динамической модели физической защиты информационных систем для анализа последствий реализации угроз, приводящих к ущербу, близкому или превышающему допустимое для данного хозяйствующего субъекта значение.

Методика проведения лабораторных работ определяется моделью решаемых задач по обеспечению физической защиты информационных объектов, исследуемых студентами на занятии по заданию преподавателя.

Средства выполнения лабораторных работ:

- программный комплекс «Эксперт - 2.0»;
- программный комплекс «EASI»;
- инструменты интегрального метода оценки рисков при распределении ограниченных ресурсов;
- программный комплекс «Adobe Photoshop».

Этапы выполнения лабораторных работ:

1. Постановка задачи лабораторной работы.
2. Ознакомление обучаемых с содержанием и объёмом лабораторной работы.
3. Порядок выполнения лабораторной работы.
4. Регистрация результатов и оформление отчёта о лабораторной работе.
5. Заключительная часть лабораторной работы.

Тематика лабораторных работ и задания к ним

Лабораторная работа 1.

Тема: **Выявление и анализ угроз охраняемым объектам с помощью программного комплекса «Эксперт - 2.0».**

Цель занятия: Ознакомление с программным комплексом оценки защищённости информационных систем «Эксперт - 2.0» и получение практических навыков в моделировании и оптимизации определения угроз безопасности информационным объектам, применения механизмов защиты в ходе осуществления мониторинга деятельности предприятий.

Учебные вопросы.

1. Формирование матрицы экспертных оценок с полями «механизмы защиты-угрозы» и «угрозы-эшелоны» для оценки достоверности активируемых механизмов защиты.
2. Формирование рейтинговых показателей в разрезе использования конкретных механизмов защиты и эшелонов для системы физической защиты в целом, а также показателей активности отдельных эшелонов и механизмов защиты.
3. Анализ активности системы физической защиты в разрезе использования конкретных механизмов и эшелонов защиты, формулирование предложений по улучшению рейтинга исследуемой системы.

Продолжительность занятия – 4 часа.

Задание на лабораторную работу №1:

1. Ознакомиться с системой показателей для оценки информационной защищённости исследуемых объектов.

2. Запустить программу «Эксперт - 2.0» и в интерактивном режиме сформировать перечень известных угроз, механизмов защиты и расставить их в иерархии эшелонов защиты для исследуемых объектов.

3. Сформировать матрицы экспертных оценок «Механизмы защиты – Угрозы» и «Угрозы – Эшелоны защиты» для повышения достоверности исходных данных и активации механизмов защиты.

4. Провести расчёт матрицы, определяющей распределение относительного потенциального ущерба по механизмам защиты и эшелонам безопасности на заданном множестве известных угроз.

5. Проанализировать активность системы информационной безопасности в разрезе использования конкретных механизмов защиты и эшелонов безопасности исследуемого предприятия.

6. Действия пунктов 3-5 повторить для различных частот активизации угроз безопасности.

7. Сформировать рейтинговые показатели при использовании конкретных механизмов защиты и эшелонов информационной безопасности для указанных информационных объектов, а также показатели активности отдельных эшелонов и механизмов защиты.

8. Создать отчёт по лабораторной работе и сформулировать выводы.

Лабораторная работа 2.

Тема: **Исследование системы физической защиты с помощью программного комплекса «Эксперт – 2.0».**

Цель занятия: Ознакомление с программным комплексом оценки защищённости информационных систем «Эксперт - 2.0» и получение практических навыков в моделировании и оптимизации применения механизмов защиты для деятельности отдельных предприятий с учётом рисков и неопределённости внешней среды.

Учебные вопросы.

1. Корректировка матрицы экспертных оценок для достоверности активации механизмов защиты с расчётом матрицы, определяющей распределение достоверности активации по механизмам защиты и эшелонам безопасности для системы физической защиты на заданном множестве известных угроз.
2. Формирование рейтинговых показателей в разрезе использования конкретных механизмов защиты и эшелонов безопасности для системы физической защиты в целом, а также показателей активности отдельных эшелонов и механизмов защиты.
3. Анализ информационной защищенности исследуемых объектов с определением конкретных механизмов защиты, обеспечивающих наибольшую динамику рейтинговых показателей.

Продолжительность занятия – 4 часа.

Задание на лабораторную работу №2:

1. Ознакомиться с системой показателей для оценки защищённости исследуемых объектов в деятельности отдельных предприятий с учётом рисков и неопределённости внешней среды.

2. Запустить программу «Эксперт - 2.0» в интерактивном режиме, получить от преподавателя вариант многоуровневой системы защиты исследуемого объекта предприятия с индивидуальным распределением конкретных механизмов защиты по эшелонам безопасности.

3. Провести расчёт матрицы, определяющей распределение относительного ущерба по механизмам защиты и уровням адаптивной системы защищённости исследуемых объектов предприятия на заданном множестве известных угроз.

4. Проанализировать активность адаптивной защиты в разрезе использования конкретных механизмов защиты и эшелонов безопасности исследуемых объектов предприятия.

5. Сформировать рейтинговые показатели в разрезе использования конкретных механизмов защиты и эшелонов безопасности исследуемых объектов предприятия.

6. Проанализировать существующую защищённость и сформулировать предложения по улучшению рейтинга системы физической защиты исследуемых объектов предприятия в рамках реализации адаптивной системы защиты.

7. Создать отчёт по лабораторной работе и сформулировать выводы.

Лабораторная работа 3.

Тема: **Исследование эффективности системы физической защиты предприятия по предполагаемым действиям нарушителя при определённых угрозах и состоянии элементов защиты с помощью программного комплекса оценки враждебных проникновений и действий "EASI".**

Цель занятия: Ознакомление студентов с комплексом показателей для оценки защищённости объектов предприятий и программным комплексом оценки враждебных проникновений и действий "Estimate of Adversary Sequence Interruption" (EASI), а так же получение практических навыков в моделировании применения механизмов физической защиты и оценки их эффективности на заданном пути нарушителя при определённых угрозах и состоянии самой системы защиты предприятия.

Учебные вопросы.

1. Анализ пути нарушителя при продвижении к охраняемому объекту.
2. Определение критической точки обнаружения и её влияние на параметры оценки прерывания последовательности действий нарушителя.
3. Построение и исследование диаграммы последовательности действий нарушителя для конкретной зоны охраняемого объекта.

Продолжительность занятия – 4 часа.

Задание на лабораторную работу №3:

1. Ознакомиться с краткими теоретическими сведениями по оценке физической защищённости охраняемых объектов и основными способами действий злоумышленников.

2. Ознакомиться с методикой применения модели "EASI" по оценке враждебных проникновений и действий нарушителя на охраняемых объектах.

3. Запустить модель "EASI" на персональном компьютере и смоделировать в интерактивном режиме возможные действия нарушителя на предложенном охраняемом объекте с выбором определённых процедур и механизмов защиты.

4. Рассчитать основные показатели эффективности по введённым данным для выбранного пути проникновения нарушителя и сформированной системы защиты охраняемого объекта, оценить её значение.

5. Проанализировать эффективность исходной системы физической защиты охраняемого объекта, выявить её недостатки и сформировать дополнительные мероприятия и средства защиты на пути проникновения нарушителя для повышения основных критериев безопасности все данные занести в рабочую таблицу модели.

6. Оценить эффективность усовершенствованной системы защиты на основе добавленных элементов на охраняемом объекте, обосновать Ваши решения расчётами с занесением данных в рабочую таблицу модели и сформировать

итоговые показатели эффективности системы физической защиты.

7. Создать отчёт по лабораторной работе и сформулировать выводы.

Лабораторная работа 4.

Тема: **Исследование системы физической защиты и охраняемых объектов с помощью интегрального метода оценки рисков при распределении ограниченных ресурсов, имеющихся в распоряжении службы безопасности.**

Цель занятия: Изучение принципов компьютерного моделирования эффективности системы физической защиты на основе общего уравнения для расчёта рисков охраняемого объекта и получение практических навыков в работе со специализированными программными средствами защиты.

Учебные вопросы.

1. Использование общего уравнения для расчёта рисков охраняемого объекта как важного инструмента количественной оценки системы физической защиты.
2. Анализ и оценка рисков для выбора оптимального варианта защиты, допустимого для охраняемого объекта по критерию затраты-прибыль в исследуемой системе физической защиты.

Продолжительность занятия – 4 часа.

Задание на лабораторную работу №4:

1. Ознакомиться с инструментом количественной оценки системы физической защиты на основе общего уравнения для расчёта рисков охраняемого объекта.

2. Сформировать рейтинговые показатели риска в разрезе использования выбранных механизмов защиты для охраняемых объектов и для системы в целом, а также показатели активности отдельных элементов защиты.

3. Воспользовавшись инструментом количественной оценки системы физиической защиты на основе общего уравнения расчёта рисков проанализировать исходную защищенность исследуемого объекта, выделить конкретные механизмы защиты, обеспечивающие наибольшую динамику рейтинговых показателей риска.

4. Сохранить в файле текущее состояние адаптивной системы физической защиты и показатели риска для дальнейших исследований.

5. Сравнить разнородную структуру системы физической защиты и рейтинговые показатели риска для заданных вариантов адаптивной защиты охраняемых объектов.

6. Результаты работы и итогового анализа сравнения поместить в Вашу папку на ПК.

7. Создать отчёт по лабораторной работе и сформулировать выводы.

4. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	**.Интеллектуальная промышленная собственность и патентное право;**	***Подготовка докладов по темам:*** 1. . Объекты и субъекты промышленной собственности. 2. Оформление прав правообладателя. 3. Объем правовой охраны, представляемый патентом.
2.	**Основные принципы и приемы инженерного творчества;**	***Подготовка докладов по темам:*** 1. Неалгоритмизированные методы инженерного творчества. 2. Алгоритмизированные методы инженерного творчества. 3. Инженер как субъект труда и жизни.
3	**Защита субъекта профессиональной деятельности в процессе его труда.**	***Подготовка докладов по темам:*** 1. Виды и ступени инженерного творчества. 2. Интеллектуальное право на результаты интеллектуальной деятельности.

5. Указания по проведению контрольных работ

5.1. Требования к структуре

Структура контрольной работы должна способствовать раскрытию темы: иметь титульный лист, содержание, введение, основную часть, заключение, список литературы.

5.2. Требования к содержанию (основной части)

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.
2. При определении целей и задач исследования необходимо правильно их формулировать. Так, в качестве цели не следует употреблять глагол «сделать». Правильно будет использовать глаголы «раскрыть», «определить», «установить», «показать», «выявить» и т.д.
3. Основная часть работы включает 2-4 вопроса, каждый из которых посвящается решению задач, сформированных во введении, и заканчивается констатацией итогов.
4. Приветствуется иллюстрация содержания работы таблицами, графическим материалом (рисунками, схемами и т.п.).
5. Необходимо давать ссылки на используемую литературу.

6. Заключение должно содержать сделанные автором работы выводы, итоги исследования.

7. Вслед за заключением идет список литературы, который должен быть составлен и оформлен с установленными требованиями. Если в работе имеются приложения, они оформляются на отдельных листах, и должны быть соответственно пронумерованы.

5.3. Требования к оформлению

Объём контрольной работы – 5-6 страниц формата А 4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

5.4. Примерная тематика контрольных работ:

1.Понятия, виды и формы «информационно-психологических воздействий» в сфере безопасности граждан и общества.

2.Информационно-психологическое оружие в современных условиях развития информационного общества.

3.Информационно-психологическая война в системе современных информационных войн.

4.Объект и субъект обеспечения информационно-психологической безопасности.

5.Принципы обеспечения информационно-психологической безопасности.

6.Основные направления обеспечения информационно-психологической безопасности фирмы.

7.Правовое регулирование обеспечения информационно-психологической безопасности граждан РФ.

8.Функции государственной системы обеспечения информационно-психологической безопасности в РФ.

9.Понятия «информационно-психологическая безопасность» в сфере безопасности предприятия.

10.Сущность информационно-психологической безопасности персонала в деятельности службы информационной безопасности предприятии.

11.Психика человека и его сознание как субъекты информационно-психологического воздействия (информационная защищенность и уязвимость).

12.Групповое и корпоративное сознание как субъекты информационно-психологического воздействия (информационная защищенность и уязвимость).

13.Психология массовой информационной коммуникации как субъекты информационно-психологического воздействия (информационная защищенность и уязвимость).

14.Признаки информационно-психологического состояния человека: национально-психологические признаки; индивидуально-личностные признаки и групповые информативные признаки.

15.Содержание и задачи по обеспечению информационно-психологической безопасности персонала и коллектива в системе безопасности предприятия.

16.Психика человека и его подсознание как субъекты информационно-психологическ

17.Определение понятия информационно-психологическое оружие и его объекты воздействия.

18.Источники поступления угроз в системе информационно-психологической безопасности предприятия.

19.Модель информационно-психологического воздействия на психику человека.

20.Общая классификация информационно-психологического оружия.

21.Характеристика MASS-MEDIA- оружие (оружие массовой информации).

22.Характеристика виртуального информационно-психологического оружия.

23.Характеристика энергоинформационно-психологического оружия.

24.Психотронно-информационное и психотропно-информационное оружие.

25.Характеристика биоэнергоинформационного оружия.

26.Информационно-генетическое и соматропно-психоинформационное оружие.

27.Лингвистическое и нейролингвистическое (программное) оружие.

28.Информационно-психологическое оружие: электронные (виртуальные) деньги и «Флэш-моб» (внезапная толпа).

29.Информационно-психологическая защита человека и коллектива: определение, объект и предмет информационно-психологической защиты.

30.Основы организации информационно-психологической безопасности на предприятии.

6. Перечень основной и дополнительной учебной литературы

Основная литература:

1.Информационно-психологическая безопасность : учебно-методическое пособие / составитель С. Ю. Махов. — Орел : МАБИВ, 2020. — 135 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176395 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

2.Психологическая безопасность : учебно-методическое пособие / составитель С. Ю. Махов. — Орел : МАБИВ, 2020. — 170 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176396 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

3.Высочина, Н. Л. Психологическое обеспечение подготовки спортсменов в олимпийском спорте : монография / Н. Л. Высочина. — Москва : Спорт-Человек, 2021. — 304 с. — ISBN 978-5-907225-44-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/165156 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

7 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Интернет-ресурсы:

1. http://eup.ru/catalog/all-all.asp – научно-образовательный портал.
2. http://informika.ru/ – образовательный портал
3. www.wikIsec.ru - Энциклопедия информационной безопасности. – Публикации, статьи.
4. **www.biblioclub.ru** - Универсальная библиотека онлайн
5. **www.rucont.ru** - ЭБС «Руконт».
6. http://www.academy.it.ru/ – академия АЙТИ.
7. http://www.minfin.ru - Официальный сайт Министерства финансов Российской Федерации
8. http://www.gov.ru/ - Официальный сервер органов государственной власти Российской Федерации.
9. http://www.fsb.ru/ - Официальный сайт Федеральной Службы Безопасности

10. http://www.fstec.ru/ - Официальный сайт Федеральной Службы по Техническому Экспортному Контролю

8. Перечень информационных технологий

Перечень программного обеспечения: *MSOffice, Multisim.*

Информационные справочные системы:

1. Электронные ресурсы образовательной среды Университета.

2. Рабочая программа и методическое обеспечение по дисциплине «Информационно-психологическая безопасность персонала предприятия».