МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ ЧЕЛЯБИИНСКОЙ ОБЛАСТИ
государственное бюджетное профессиональное образовательное учреждение
«Магнитогорский педагогический колледж»

СОГЛАСОВАНО:
Педагогическим советом
Протокол № 1 от 31.08.2023г.
Председатель Педагогического совета:
_____ /О.Ю. Леушканова/

Научно-методическим советом
Протокол № 1 от 01.09.2023 г.
Председатель Научно-методического совета:
_____ /Е.Ю. Иванова/

УТВЕРЖДЕНО
Приказом № 199 от 28.06.2023 г.

Директор государственного бюджетного профессионального образовательного учреждения «Магнитогорский педагогический колледж»
_____ /О.Ю. Леушканова/

ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ОБЩЕРАЗВИВАЮЩАЯ ПРОГРАММА

«Введение в специальность. Кибербезопасность.»

социально- гуманитарной направленности

Уровень сложности: базовый

Срок обучения: 36 часов (8 месяцев)

Форма обучения: очная

Разработчик: Понкратова М. В., преподаватель

Магнитогорск 2023 г.

Содержание

1. Основные характеристики программы

Общая характеристика

Развитие информационного общества предполагает внедрение информационных технологий во все сферы жизни, но это означает и появление новых угроз безопасности – от утечек информации до кибертерроризма. В проекте Концепции стратегии кибербезопасности Российской Федерации киберпространство определяется как «сфера деятельности в информационном пространстве, образованная совокупностью Интернета и других телекоммуникационных сетей и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства)», а кибербезопасность – как «совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями». В связи с этим большое значение приобретает проблема «культуры безопасного поведения в киберпространстве».

В соответствии со «Стратегией развития отрасли информационных технологий в Российской Федерации на 2014-2020 годы и на перспективу до 2025 года», утвержденной распоряжением Правительства Российской Федерации от 1 ноября 2013 г. № 2036-р (в ред. распоряжения Правительства РФ от 18.10.2018 N 2253-р), Указом Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» и рядом других документов в числе многих других задач выделяются:

- обеспечение различных сфер экономики качественными информационными технологиями;
- обеспечение высокого уровня информационной безопасности государства, индустрии и граждан.

Безопасность в информационном обществе является одним из основных направлений фундаментальных исследований в области информационных технологий. Киберугрозы существуют везде, где применяются

информационные технологии.

Курс дополнительной общеобразовательной общеразвивающей программы «введение в специальность. Кибербезопасность» является дополнительным в общей системе подготовки специалиста, он логически связан с профессиональными модулями.

Нормативно-правовые документы по проектированию и реализации дополнительных общеобразовательных (общеразвивающих) программ

При разработке дополнительных общеобразовательных (общеразвивающих) программ (ДООП) педагоги дополнительного образования руководствуются следующей нормативной базой: документами, размещенными по ссылке http://оирo.рф/wpcontent/uploads/2023/06/Normativno-pravovye-osnovy-realizacii-DOOP.docx

Актуальные документы:

- Федеральный закон Российской Федерации от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» (с изменениями на 17 февраля 2023 года) (далее – Федеральный закон);
- Концепция развития дополнительного образования детей до 2030 года (от 31 марта 2022 года № 678-р) (далее – Концепция);
- Приказ Министерства просвещения Российской Федерации т 27.07.2022 № 629 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»

Категория слушателей:	Студенты 1 курса колледжа по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем»

2. Цель, задачи и планируемые результаты обучения по дополнительной общеобразовательной общеразвивающей программе

Цель программы – создание условий для формирования у слушателей цифровой культуры личности с необходимыми навыками и присущими ценностями, взглядами, ориентациями, установками, мотивами деятельности и поведения для обеспечения безопасной и развивающей жизнедеятельности студента в сети «Интернет».

Для достижения поставленной цели решаются следующие **задачи**:

- Формирование у слушателей цифровой и информационной культуры;
- Воспитание у студентов нравственности и культуры взаимоотношения с людьми на основе общечеловеческих ценностей в сети «Интернет»;
- Утверждение в сознании и чувствах студентов правильных моделей поведения, ценностей, взглядов и убеждений для успешной жизнедеятельности студента в сети «Интернет»;
- Интеллектуальное развитие студентов, развитие творческих и прикладных качеств мышления;
- Развитие интереса к различным сферам информационных технологий;
- Совершенствование навыков самообразования, всестороннего развития и социализации;
- Обучение поиску и отбору информации, её интерпретации и применимости;
- Развитие логического мышления, умений обобщения и конкретизации, анализа и синтеза;

Планируемые результаты обучения

В результате освоения программы обучающийся должен знать:

- сущность и понятие информационной безопасности, характеристику ее составляющих;
- место информационной безопасности в системе национальной безопасности страны;

- источники угроз информационной безопасности и меры по их предотвращению;
- жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи;
- современные средства и способы обеспечения информационной безопасности.

Объём программы – 36 академических часов, нормативный срок освоения – 8 месяцев.

Форма обучения – очная

Режим занятий: 36 недель, 1 занятие в неделю, продолжительность одного занятия 1 академический час.

Принципы формирования групп – по желанию обучающихся или по выбору педагога. Количество человек в группе – от 15 до 30.

Форма организации образовательного процесса: групповая.

Форма оценивания планируемых результатов: по итогам освоения данной программы после успешного прохождения итогового контроля в виде **зачета** в письменной форме слушатели получают сертификат об обучении установленного образца в объеме 36 академических часов.

3. Учебный план

Уровень сложности	№	Разделы	Трудоемкость			Формы аттестации
			Всего	Теория	Практика	
Базовый	**1**	**Общие сведения о безопасности ПК и Интернета**	**11**	11	0	-
	1.1	Защита киберпространства как комплекс мероприятий, направленных на обеспечение информационной безопасности. Аспекты кибербезопасности.	**1**	1	0	-
	1.2	Компьютерная и информационная безопасность, обнаружение проблем сети, восстановление параметров систем, средства защиты от несанкционированного доступа к данным, криптографическая защита информации.	**1**	1	0	-
	1.3	Что такое защищенная информационная среда. Защита каналов передачи данных, Средства предотвращения утечки информации, защита информации от НСД (антивирусная защита, средства контроля защищенности, средства обнаружения и Предупреждения атак), средства аутентификации.	**1**	1	0	-
	1.4	Организационно-технические меры защиты информационной среды. Системы охранной сигнализации, видеонаблюдение, контроль и управление доступом, средства уничтожения информации, средства резервного копирования и восстановления.	**1**	1	0	-
	1.5	Требования к безопасности информации: сохранение целостности, Конфиденциальности и доступности. Определения по ГОСТ РВ 51987-2002 «Информационная технология. Комплекс стандартов на автоматизированные системы. Типовые требования и показатели качества функционирования информационных систем. Общие положения».	**1**	1	0	-

Уровень сложности	№	Разделы	Трудоемкость			Формы аттестации
			Всего	Теория	Практи	
	1.6	Признаки нарушения целостности программ и данных. Способы нарушения целостности информации. Признаки и способы нарушения конфиденциальности. Признаки и способы нарушения доступности информации.	**1**	1	0	-
	1.7	Безопасность мобильных устройств в информационных системах. Источники заражения мобильных устройств (веб-ресурсы, магазины приложений, ботнеты).	**1**	1	0	-
Базовый	1.8	Угрозы безопасности в сетях WiFi. Методы защиты сетей WiFi.	**1**	1	0	-
	1.9	Угрозы информации (техногенные, случайные и преднамеренные; природные). Неосторожность пользователя как одна из угроз для информационной безопасности.	**1**	1	0	-
	1.10	Меры кибербезопасности для конечных пользователей. Использование рекомендованных версий операционных систем и приложений, использование антивирусных средств, настройка веб-браузеров, блокировка скриптов, использование фильтров фишинга, межсетевых экранов. Автоматическое обновление ПО.	**1**	1	0	-
	1.11	Киберугрозы Интернета (кибервойны, манипулирование людьми, зависимость, вирусные атаки, отсутствие приватности).	**1**	1	0	-
Базовый	**2**	**Техника безопасности и экология**	**3**	3	0	
	2.1	Кибератаки на инфраструктуру.	**1**	1	0	
	2.2	Компьютер в режиме труда и отдыха. Информационная перегрузка.	**1**	1	0	
	2.3	Влияние компьютера на репродуктивную систему.	**1**	1	0	
Базовый	**3**	**Проблемы Интернет-зависимости**	**2**	2	0	
	3.1	Типы интернет-зависимости (пристрастие к работе с компьютером, к навигации и поиску информации, игромания и электронные покупки, зависимость от	**1**	1	0	

Уровень сложности	№	Разделы	Трудоемкость			Формы аттестации
			Всего	Теория	Практика	
		сетевого общения, сексуальные зависимости).				
	3.2	Проблемы безопасности инфраструктуры Интернета (протоколы маршрутизации сети, система доменных имен, средства маршрутизации и т.п.). Методы защиты.	1	1	0	
Базовый	**4**	**Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы.**	7	7	0	
	4.1	Проблемы безопасности инфраструктуры Интернета (протоколы маршрутизации сети, система доменных имен, средства маршрутизации и т.п.). Методы защиты.	1	1	0	
	4.2	Проверка подлинности (аутентификация) в Интернете.	1	1	0	
	4.3	Меры безопасности для пользователя WiFi. Настройка безопасности.	1	1	0	
	4.4	Вирусы для мобильных устройств (мобильные банкеры и др.).	1	1	0	
	4.5	Настройка компьютера для безопасной работы.	1	1	0	
	4.6	Ошибки пользователя (установка нескольких антивирусов, установка слишком большого числа программ, отсутствие резервного копирования и т.п.).	1	1	0	
	4.7	Меры личной безопасности при сетевом общении. Настройки приватности в социальных сетях.	1	1	0	
Базовый	**5**	**Мошеннические действия в Интернете. Киберпреступления.**	7	7	0	
	5.1	Мошеннические действия в сети. Предложения о разблокировании программ (блокировщики windows). Ложные антивирусы.	1	1	0	
	5.2	Подмена страниц в интернете (сайты-клоны). Фальшивые файлообменники.	1	1	0	
	5.3	Мошеннические действия в сети. Сбор «пожертвований» на благотворительность. «Легкий заработок» в Интернете. Пирамиды.	1	1	0	
	5.4	Что такое электронный кошелек –	1	1	0	

Уровень сложности	№	Разделы	Трудоемкость			Формы аттестации
			Всего	Теория	Практика	
		удобства и проблемы безопасности. «Обменники» для электронных денег.				
	5.5	Мошенничество при распространении «бесплатного» ПО. Продажа «обучающих курсов» для бизнеса.	**1**	1	0	
	5.6	Платные предложения работы. Платный просмотр видеоматериалов.	**1**	1	0	
	5.7	Технологии манипулирования в Интернете.	**1**	1	0	
Базовый	**6**	**Сетевой этикет. Психология и сеть.**	**2**	2	0	
	6.1	Безопасная работа в сети в процессе сетевой коммуникации (чаты, форумы, конференции, скайп, социальные сети и пр.). Сетевой этикет. Термины сетевого этикета: оверквотинг, флейм, флуд, оффтопик, смайлики и др.	**2**	2	0	
Базовый	**7**	**Правовые аспекты защиты киберпространства.**	**4**	2	2	
		Как расследуются преступления в сети.	**1**	1	0	
		Ответственность за интернет-мошенничество.	**1**	1	0	
		Обобщение материала курса "Зачётная работа"	**2**	0	2	Зачетная Работа
		ВСЕГО:	**36**	32	4	

4. Календарный учебный график

I полугодие 2023 – 2024 учебный год

Курс	Индекс	Наименование циклов, разделов, дисциплин, профессиональных модулей, МДК, практик	Виды учебной нагрузки	01.09 - 07.09	08.09 - 14.09	15.09 - 21.09	22.09 - 28.09	29.09 - 05.10	06.10 - 12.10	13.10 - 19.10	20.10 - 26.10	27.10 - 02.11	03.11 - 09.11	10.11 - 16.11	17.11 - 23.11	24.11 - 30.11	01.12 - 07.12	08.12 - 14.12	15.12 - 21.12	22.12 - 28.12	Всего часов	29.12 - 04.01	05.01 - 11.01
				сентябрь				октябрь				ноябрь					декабрь						
				35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51		52	01
				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	-	18	19
1 курс			**обяз.уч.**	**0**	**0**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**15**		
			обяз.уч.	**0**	**0**	***1***	***1***	***1***	***1***	***1***	***1***	***1***	***1***	***1***	***1***	***1***	***1***	***1***	***1***	***1***	**15**		
		Введение в специальность. Кибербезопасность	обяз.уч.			1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	***15***	К	К
Всего час.в неделю обязательной нагрузки				**0**	**0**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**15** ***15***		
Всего часов в неделю				**0**	**0**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**15**		

К - каникулы

Календарный учебный график

II полугодие 2023 – 2024 учебный год

Курс	Индекс	Наименование циклов, разделов, дисциплин, профессиональных модулей, МДК, практик	Виды учебной нагрузки		29.12 - 04.01	05.01 - 11.01	12.01 - 18.01	19.01 - 25.01	26.01 - 01.02	02.02 - 08.02	09.02 - 15.02	16.02 - 22.02	23.02 - 29.02	01.03 - 07.03	08.03 - 14.03	15.03 - 21.03	22.03 - 28.03	29.03 - 04.04	05.04 - 11.04	12.04 - 18.04	19.04 - 25.04	26.04 - 02.05	03.05 - 09.05	10.05 - 16.05	17.05 - 23.05	24.05 - 30.05	31.05 - 06.06		Всего часов
					январь					февраль				март					апрель				май				июнь		
					52	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22		
					18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40		
1 курс			обяз.уч.				1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	0	21	36
			обяз.уч.				*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*2*	*0*	21	36
		Введение в специальность. Кибербезопасность	обяз.уч.		К	К	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2		21	36
		Всего час.в неделю обязательной нагрузки																										21	36
					К	К	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	0	21	36
		Всего часов в неделю					1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	0	21	36

К - каникулы

5. Содержание программы

Раздел 1. Общие сведения о безопасности ПК и Интернета (11 часов).

Защита киберпространства как комплекс мероприятий, направленных на обеспечение информационной безопасности. Аспекты кибербезопасности.

Компьютерная и информационная безопасность, обнаружение проблем сети, восстановление параметров систем, средства защиты от несанкционированного доступа к данным, криптографическая защита информации.

Что такое защищенная информационная среда. Защита каналов передачи данных, средства предотвращения утечки информации, защита информации от НСД (антивирусная защита, средства контроля защищенности, средства обнаружения и предупреждения атак), средства аутентификации.

Организационно-технические меры защиты информационной среды. Системы охранной сигнализации, видеонаблюдение, контроль и управление доступом, средства уничтожения информации, средства резервного копирования и восстановления.

Требования к безопасности информации: сохранение целостности, конфиденциальности и доступности. Определения по ГОСТ РВ 51987-2002 «Информационная технология. Комплекс стандартов на автоматизированные системы. Типовые требования и показатели качества функционирования информационных систем. Общие положения».

Признаки нарушения целостности программ и данных. Способы нарушения целостности информации. Признаки и способы нарушения конфиденциальности. Признаки и способы нарушения доступности информации.

Безопасность мобильных устройств в информационных системах. Источники заражения мобильных устройств (веб-ресурсы, магазины

приложений, ботнеты).

Угрозы безопасности в сетях WiFi. Методы защиты сетей WiFi.

Угрозы информации (техногенные, случайные и преднамеренные; природные). Неосторожность пользователя как одна из угроз для информационной безопасности.

Меры кибербезопасности для конечных пользователей. Использование рекомендованных версий операционных систем и приложений, использование антивирусных средств, настройка веб-браузеров, блокировка скриптов, использование фильтров фишинга, межсетевых экранов. Автоматическое обновление ПО.

Киберугрозы Интернета (кибервойны, манипулирование людьми, зависимость, вирусные атаки, отсутствие приватности).

Раздел 2. Техника безопасности и экология (3 часа).

Кибератаки на инфраструктуру. Компьютер в режиме труда и отдыха. Информационная перегрузка. Влияние компьютера на репродуктивную систему.

Раздел 3. Проблемы Интернет-зависимости (2 часа).

Интернет- и компьютерная зависимость (аддикция). Критерии зависимости с точки зрения психологов (приоритетность, изменения настроения, толерантность, симптом разрыва, конфликт, рецидив). Как развивается зависимость.

Типы интернет-зависимости (пристрастие к работе с компьютером, к навигации и поиску информации, игромания и электронные покупки, зависимость от сетевого общения, сексуальные зависимости).

Раздел 4. Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы (7 часов).

Проблемы безопасности инфраструктуры Интернета (протоколы маршрутизации сети, система доменных имен, средства маршрутизации и т.п.). Методы защиты.

Проверка подлинности (аутентификация) в Интернете. Меры безопасности для пользователя WiFi. Настройка безопасности.

Вирусы для мобильных устройств (мобильные банкеры и др.).

Настройка компьютера для безопасной работы. Ошибки пользователя

(установка нескольких антивирусов, установка слишком большого числа программ, отсутствие резервного копирования и т.п.).

Меры личной безопасности при сетевом общении. Настройки приватности в социальных сетях.

Раздел 5. Мошеннические действия в Интернете. Киберпреступления (7часов).

Мошеннические действия в сети. Предложения о разблокировании программ (блокировщики windows). Ложные антивирусы.

Подмена страниц в интернете (сайты-клоны). Фальшивые файлообменники.

Мошеннические действия в сети. Сбор «пожертвований» на благотворительность. «Легкий заработок» в Интернете. Пирамиды.

Что такое электронный кошелек – удобства и проблемы безопасности. «Обменники» для электронных денег.

Мошенничество при распространении «бесплатного» ПО. Продажа «обучающих курсов» для бизнеса.

Платные предложения работы. Платный просмотр видеоматериалов.

Технологии манипулирования в Интернете.

Раздел 6. Сетевой этикет. Психология и сеть (2 часа).

Безопасная работа в сети в процессе сетевой коммуникации (чаты, форумы, конференции, скайп, социальные сети и пр.). Сетевой этикет. Термины сетевого этикета: оверквотинг, флейм, флуд, оффтопик, смайлики и др.

Раздел 7. Правовые аспекты защиты киберпространства (4 часа).

Как расследуются преступления в сети. Ответственность за интернет-мошенничество. Обобщение материала курса «Зачетная работа»

6. Организационно – педагогические условия

Все занятия осуществляются в лекционно-семинарской форме с помощью визуальных и информационно-коммуникационных технологий.

Используются материалы электронной библиотеки образовательной платформы Юрайт, сайта «Лаборатория Касперского», видеохостинга YouTube.

Материально-технические условия реализации программы

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
Аудитория 233	Лекции, семинары	Ноутбуки, автоматизированное рабочее место, проектор, экран, принтер

7. Форма аттестации

Оценка качества освоения программы осуществляется преподавателем в виде зачетной работы в письменной форме. Слушатель считается аттестованным, если ответил правильно на 50% заданий.

8. Оценочные и методические материалы и иные компоненты

Зачётная работа «Введение в специальность. Кибербезопасность.»

1. Под информационной безопасностью понимается…

А) **защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре.**

Б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия

В) нет правильного ответа

2. Защита информации – это..

А) **комплекс мероприятий, направленных на обеспечение информационной безопасности.**

Б) процесс разработки структуры базы данных в соответствии с требованиями пользователей

В) небольшая программа для выполнения определенной задачи

3. От чего зависит информационная безопасность?

А) **от компьютеров**

Б) от поддерживающей инфраструктуры

В) от информации

4. Основные составляющие кибербезопасности:

А) целостность

Б) достоверность

В) конфиденциальность

5. Доступность – это…

А) **возможность за приемлемое время получить требуемую информационную услугу.**

Б) логическая независимость

В) нет правильного ответа

6. Целостность – это..

А) **целостность информации**

Б) непротиворечивость информации

В) защищенность от разрушения

7. Конфиденциальность – это..

А) **защита от несанкционированного доступа к информации**

Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов

В) описание процедур

8. Для чего создаются информационные системы?

А) **получения определенных информационных услуг**

Б) обработки информации

В) все ответы правильные

9. Целостность можно подразделить:

А) **статическую**

Б) динамичную

В) структурную

10. Где применяются средства контроля динамической целостности?

А) **анализе потока финансовых сообщений**

Б) обработке данных

В) **при выявлении кражи, дублирования отдельных сообщений**

11. Какие трудности возникают в информационных системах при конфиденциальности?
А) сведения о технических каналах утечки информации являются закрытыми
Б) на пути пользовательской криптографии стоят многочисленные технические проблемы
В) **все ответы правильные**
12. Угроза – это…
А) **потенциальная возможность определенным образом нарушить информационную безопасность**
Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа
13. Атака – это…
А) **попытка реализации угрозы**
Б) потенциальная возможность определенным образом нарушить информационную безопасность
В) программы, предназначенные для поиска необходимых программ.
14. Источник угрозы – это..
А) **потенциальный злоумышленник**
Б) злоумышленник
В) нет правильного ответа
15. Окно опасности – это…
А) **промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется.**
Б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области
В) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере
16. Какие события должны произойти за время существования окна опасности?
А) **должно стать известно о средствах использования пробелов в защите.**
Б) должны быть выпущены соответствующие заплаты.

В) заплаты должны быть установлены в защищаемой И.С.
17. Угрозы можно классифицировать по нескольким критериям:
А) **по спектру И.Б.**
Б) по способу осуществления
В) по компонентам И.С.
18. По каким компонентам классифицируется угрозы доступности:
А) **отказ пользователей**
Б) отказ поддерживающей инфраструктуры
В) ошибка в программе
19. Основными источниками внутренних отказов являются:
А) отступление от установленных правил эксплуатации
Б) разрушение данных
В) **все ответы правильные**
20. Основными источниками внутренних отказов являются:
А) **ошибки при конфигурировании системы**
Б) отказы программного или аппаратного обеспечения
В) выход системы из штатного режима эксплуатации
21. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:
А) **невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности**

Б) обрабатывать большой объем программной информации
В) нет правильного ответа
22. Какие существуют грани вредоносного П.О.?
А) **вредоносная функция**
Б) внешнее представление
В) способ распространения
23. По механизму распространения П.О. различают:
А) вирусы
Б) черви
В) **все ответы правильные**
24. Вирус – это…
А) **код обладающий способностью к распространению путем внедрения в другие программы**
Б) способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов
В) небольшая программа для выполнения определенной задачи
25. Черви – это…
А) **код способный самостоятельно, то есть без внедрения в другие программы вызывать распространения своих копий по И.С. и их выполнения**
Б) код обладающий способностью к распространению путем внедрения в другие программы
В) программа действий над объектом или его свойствами
26. Конфиденциальную информацию можно разделить:
А) **предметную**
Б) служебную
В) глобальную
27. Природа происхождения угроз:
А) **случайные**
Б) преднамеренные
А) **объективные**
Б) субъективные
В) преднамеренные
28. К какому виду угроз относится присвоение чужого права?
А) **нарушение права собственности**
Б) нарушение содержания
В) внешняя среда
29. Отказ, ошибки, сбой – это:
А) **случайные угрозы**
Б) преднамеренные угрозы
В) природные угрозы
30. Отказ - это…
А) **нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций**
Б) некоторая последовательность действий, необходимых для выполнения конкретного задания
В) структура, определяющая последовательность выполнения и взаимосвязи процессов
31. Ошибка – это…
А) **неправильное выполнение элементом одной или нескольких функций происходящее в следствии специфического состояния**
Б) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
В) негативное воздействие на программу
32. Сбой – это…

А) **такое нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент**
Б) неправильное выполнение элементом одной или нескольких функций происходящее в следствие специфического состояния
В) объект-метод
33. Побочное влияние – это…
А) **негативное воздействие на систему в целом или отдельные элементы**
Б) нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
В) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
34. СЗИ (система защиты информации) делится:
А) **ресурсы автоматизированных систем**
Б) организационно-правовое обеспечение
В) человеческий компонент
35. Что относится к человеческому компоненту СЗИ?
А) **системные порты**
Б) администрация
В) программное обеспечение
36. Правовое обеспечение безопасности информации – это…
А) **совокупность законодательных актов, нормативно-правовых документов, руководств, требований, которые обязательны в системе защиты информации**
Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
В) нет правильного ответа
37. Информацию с ограниченным доступом делят:
А) **государственную тайну**
Б) конфиденциальную информацию
В) достоверную информацию
В) природные
38. Предпосылки появления угроз: (перечислите)_____

39. Что относится к государственной тайне?
А) **сведения, защищаемые государством в области военной, экономической … деятельности**
Б) документированная информация
В) нет правильного ответа
40. Вредоносная программа - это…
А) **программа, специально разработанная для нарушения нормального функционирования систем**
Б) упорядочение абстракций, расположение их по уровням
В) процесс разделения элементов абстракции, которые образуют ее структуру и поведение

СПИСОК ЛИТЕРАТУРЫ И ДРУГИХ ИСТОЧНИКОВ

Основные источники:

1. Внуков, А. А. Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2021. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст: электронный // Образовательная платформа Юрайт [сайт].

2. Корабельников, С. М. Преступления в сфере информационной безопасности: учебное пособие для вузов / С. М. Корабельников. — Москва: Издательство Юрайт, 2020. — 111 с. — (Высшее образование).
— ISBN 978-5-534-12769-0. — Текст: электронный // Образовательная платформа Юрайт [сайт].

3. Чернова, Е. В. Информационная безопасность человека: учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2020. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст: электронный // Образовательная платформа Юрайт [сайт].

Интернет-ресурсы

1. https://www.youtube.com

https://www.kaspersky.ru/resource-center