МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ
«ТЕХНОПОЛИС»

РАССМОТРЕНА
на педагогическом совете
Протокол № 2 от 15.01.2024 г.

УТВЕРЖДЕНА
Директор МАОУ ДО «Технополис»
_____Т. Г. Андроник
Приказ № ТЕХ-12-6/4
18.01.2024 г.

КРАТКОСРОЧНАЯ ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА

(СЕТЕВАЯ, ДИСТАНЦИОННАЯ)

«БЕЗОПАСНОСТЬ В СЕТИ»

Срок реализации: 3 месяца
Возраст обучающихся: 9-13 лет
Количество часов: 10
Авторский коллектив МАОУ ДО
«Технополис»

Сургут, 2024

АННОТАЦИЯ

Дополнительная общеобразовательная программа стартового уровня «Безопасность в сети» разработана в связи с возросшей потребностью обеспечения информационной безопасности детей и подростков в сети Интернет.

Срок реализации программы: 3 месяца.

Количество часов: 10 часов.

Возраст обучающихся: 9-13 лет (4-7 классы).

ПАСПОРТ ДОПОЛНИТЕЛЬНОЙ ОБЩЕОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Название программы	**Безопасность в сети**
Направленность программы	Техническая
Уровень программы	Стартовый
ФИО разработчика (составителя) программы	Куприянова Наталья Васильевна Рябошапко Елена Владимировна
Год разработки или модификации	2024
Где, когда и кем утверждена программа	Принята педагогическим советом МАОУ ДО «Технополис», протокол №2 от 15.01.2024, утверждена директором МАОУ ДО «Технополис»
Информация о наличии рецензии	нет
Цель	Освоение обучающимися базовых принципов безопасного поведения в сети интернет и безопасности личного информационного пространства
Задачи	***Обучающие:*** 1) Способствовать формированию знаний о безопасном поведении при работе с компьютерными программами, информацией в сети Интернет; 2) Формировать умения соблюдать нормы информационной этики; 3) Формировать умения безопасной работы с информацией, анализировать и обобщать полученную информацию. ***Воспитательные:*** 1) Развивать компьютерную грамотность и информационную культуру личности в использовании информационных и коммуникационных технологий; 2) Развивать умение анализировать и систематизировать имеющуюся информацию; 3) Развивать познавательную и творческую активность в безопасном использовании информационных и коммуникационных технологий. ***Развивающие:*** 1) Способствовать выработке сознательного и бережного отношения к вопросам собственной информационной безопасности; 2) Способствовать формированию и развитию нравственных, этических и патриотических качеств личности.
Планируемые результаты освоения программы	Обучающиеся должны: ***знать:*** • структуры интернет-пространства, типы источников информации и разновидностей контента; • признаки рискованного и опасного поведения и различных угроз в интернет-пространстве • правила безопасного поведения в интернет-

	пространстве, рационального использования персональных данных, защиты от вредоносных воздействий; ***уметь:*** • работать с поисковыми системами, общедоступными средствами поиска информации в интернет-пространстве • грамотно представлять в интернет-пространстве свои личные и персональные данные, формировать и поддерживать собственный позитивный имидж в социальных сетях.
Срок реализации программы	3 месяца
Возраст обучающихся	9-13 лет
Формы занятий	Лекции, практическая работа, самостоятельная работа
Методическое обеспечение	Методические рекомендации по выполнению практических работ; Методические рекомендации по выполнению самостоятельных работ
Условия реализации программы (оборудование, инвентарь, специальные помещения, ИКТ и др.)	***Материально-техническое обеспечение:*** 1. Программное обеспечение; 2. Компьютер с выделенным каналом выхода в Интернет; 3. Мультимедийная проекционная установка или интерактивная доска; 4. МФУ (принтер черно-белый, цветной; сканер, ксерокс)

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Интернет – всемирная система объединенных компьютерных сетей для хранения и передачи информации, которая главным образом предназначалась для использования правительством и государственными органами, а позже для исследовательских и образовательных сообществ. Поэтому очень важно уметь ориентироваться в этом огромном объеме информации, отличать достоверную информацию от ложной, обезопасить себя и свои личные данные от негативных действий других пользователей сети.

При разработке программы использовались нормативно-правовые документы:

1. Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;
2. Распоряжение Правительства РФ от 31.03.2022 г. № 678-р «Концепция развития дополнительного образования детей до 2030 года»;
3. Приказ Министерства просвещения РФ от 27.07.2022 N 629 «Об утверждении порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»;
4. Приказ Министерства просвещения РФ от 30.09.2020 г. № 533 «О внесении изменений в порядок организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»;
5. Постановление Главного государственного санитарного врача РФ от 28.09.2020 № 28 «Об утверждении санитарных правил СП 2.4.3648-20 «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи».
6. Федеральный закон от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребёнка в РФ»;
7. Федеральный закон от 21.11.2011 №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
8. Государственная программа Российской Федерации «Развитие образования» (утверждена Постановлением Правительства РФ от 26.12.2017 № 1642 (ред. от 22.02.2021) «Об утверждении государственной программы Российской Федерации» Развитие образования;
9. Приказ Министерства просвещения Российской Федерации от 03.09.2019 г. № 467 «Об утверждении Целевой модели развития региональных систем дополнительного образования детей» ред. от 02.02.2021г.;
10. Приказ Министерства труда и социальной защиты Российской Федерации от 22.09.2021г. № 652н «Об утверждении профессионального стандарта «Педагог дополнительного образования детей и взрослых»;
11. Приказ Министерства образования и науки Российской Федерации от 09.01.2014 г. №2 «Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»;
12. Письмо Министерства образования и науки РФ от 18.11.2015г. № 09–3242. «О направлении Методических рекомендаций по проектированию дополнительных общеразвивающих программ (включая разноуровневые)».

Реализация образовательной программы осуществляется за пределами ФГОС и федеральных государственных требований, и не предусматривает подготовку обучающихся к прохождению государственной итоговой аттестации по образовательным программам.

Направленность программы: техническая.

Уровень программы: стартовый.

Новизна программы. Безопасность в сети - это защищённость в информационном

пространстве. На занятиях обучающиеся рассмотрят структуру интернет-пространства, научатся разбираться в источниках и типах информации в интернете, освоят поисковые системы и средства поиска информации.

Актуальность. Интернет стал неотъемлемой частью жизни. В ирреальном пространстве возможно абсолютно все: приобретать товар, находить знакомых, необходимую информацию и т.д. Но часто пользователи сталкиваются с мошенничеством. Поэтому важно знать правила безопасности в интернете.

Педагогическая целесообразность данной программы заключается в пробуждении интереса обучающихся к новому виду деятельности.

Цель программы:

Формирование у обучающихся способности к разностороннему и комплексному анализу информации, размещенной на различных Интернет-ресурсах, в интересах безопасного и рационального использования интернет-пространства.

***Задачи*:**

Обучающие:

1) Способствовать формированию знаний о безопасном поведении при работе с компьютерными программами, информацией в сети Интернет;
2) Формировать умения соблюдать нормы информационной этики;
3) Формировать умения безопасной работы с информацией, анализировать и обобщать полученную информацию.

Воспитательные:

1) Развивать компьютерную грамотность и информационную культуру личности в использовании информационных и коммуникационных технологий;
2) Развивать умение анализировать и систематизировать имеющуюся информацию;
3) Развивать познавательную и творческую активность в безопасном использовании информационных и коммуникационных технологий.

Развивающие:

1) Способствовать выработке сознательного и бережного отношения к вопросам собственной информационной безопасности;
2) Способствовать формированию и развитию нравственных, этических и патриотических качеств личности.

ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ

Возраст обучающихся: 9-13 лет (4-7 класс).

Условия приема детей: на курсы программы зачисляются все желающие при наличии свободных мест.

Срок реализации программы: 3 месяца (10 часов).

Формы организации деятельности обучающихся

При изучении тем программа предусматривает использование индивидуальной и групповой формы учебной работы обучающихся, в том числе:

- интерактивные лекции;

- практическая работа.

Методы обучения

При реализации программы рекомендуется использовать следующие методы:

- проблемное изложение;
- информационный рассказ;
- иллюстрация;
- демонстрация наглядного материала;
- изучение источников;
- беседа;
- дискуссия;
- игровые ситуации;
- устный опрос.

Формы занятий: теоретические, практические, комбинированные.

Планируемые результаты

В результате освоения программы обучающийся должен приобрести следующие знания, умения и навыки:

Обучающиеся должны:

знать:

- структуры интернет-пространства, типы источников информации и разновидностей контента;
- признаки рискованного и опасного поведения и различных угроз в интернет-пространстве
- правила безопасного поведения в интернет-пространстве, рационального использования персональных данных, защиты от вредоносных воздействий;

уметь:

- работать с поисковыми системами, общедоступными средствами поиска информации в интернет-пространстве
- грамотно представлять в интернет-пространстве свои личные и персональные данные, формировать и поддерживать собственный позитивный имидж в социальных сетях.

Формы подведения итогов реализации программы

Контроль знаний и умений учащихся можно осуществлять в выполнения практических работ и тестовых заданий после изучения каждой темы.

По окончании обучения итоговая аттестация проводится на основе выполнения тестовых заданий.

Методическое обеспечение дополнительной общеобразовательной программы «Безопасность в сети»

При реализации программы рекомендуется применять следующие методы обучения: объяснительно-иллюстративный, репродуктивный, метод проблемного изложения, частично-поисковый (эвристический) метод. Педагогам, работающим по данной программе, необходимо учитывать стартовые позиции каждого ученика и осуществлять индивидуальный подход за счет разноуровневых заданий. Целесообразно использовать блок-схемы для повышения наглядности при демонстрации элементарных алгоритмов.

В целом, методическое сопровождение данной программы реализуется за счет использования в образовательном процессе дидактических материалов: методические разработки педагога (педагогов, работающих по данной программе), авторские презентации, Интернет-ресурсы, интерактивные задания, литература для педагога и обучающихся.

Формы проведения занятий в рамках программы:

- Интерактивные лекции;
- Практическая работа;
- Самостоятельная работа учащихся (индивидуально и в малых группах).

Материально-техническое обеспечение:

1. Программное обеспечение;
2. Компьютер с выделенным каналом выхода в Интернет;
3. Мультимедийная проекционная установка или интерактивная доска;
4. МФУ (принтер черно-белый, цветной; сканер, ксерокс)

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН

№	Наименование кейса, темы	Количество часов			Форма аттестации /контроля
		Всего	Теория	Практика	
1.	Тема 1. Информационная структура интернета, поисковые системы. Принципы эффективного поиска информации в интернете.	**1**	1		Собеседование
2.	Тема 2. Социальные сети и социальные медиа, поведение молодежи в сети, проблема лайков.	1	1		Собеседование
3.	Тема 3. Фейковые сообщения и вредоносное ПО в сети Интернет.	**1**		1	Практическая работа
4.	Тема 4. Проблемы хакерства.	**1**	1		Собеседование
5.	Тема 5. Проблема краж персональных данных с помощью вредоносного ПО	**1**	1		Собеседование
6.	Тема 6. Изучение структуры сообщества, авторов сообщений в социальной сети «ВКонтакте».	**1**		1	Практическая работа
7.	Тема 7. Правила функционирования сетевых сообществ. Правила сетевого общения.	**1**	1		Собеседование
8.	Тема 8. Защищенность данных в сети. Проблемы утечки данных. Проблемы использования в сообщениях геотегов, столкновения с неразумным и агрессивным поведением в сети.	**1**		1	Практическая работа
9.	Тема 9. Благотворительность с помощью интернет. Риски потребительского поведения.	**1**		1	Практическая работа
10.	Тема 10. Проблема оказания поддельных услуг и распространения подозрительных объявлений об удаленной работе в социальных сетях.	**1**		**1**	Практическая работа
	Итого	**10**	**5**	**5**	

КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

№ п/п	Месяц	Число	Время поведения занятия	Форма занятия	Кол-во часов	Тема занятия	Место проведения	Форма контроля
1.				Теория	1	Тема 1. Информационная структура интернета, поисковые системы. Принципы эффективного поиска информации в интернете.	Кванториум	Собеседование
2.				Теория	1	Тема 2. Социальные сети и социальные медиа, поведение молодежи в сети, проблема лайков.	Кванториум	Собеседование
3.				Практическая работа	1	Тема 3. Фейковые сообщения и вредоносное ПО в сети Интернет.	Кванториум	Практическая работа
4.				Теория	1	Тема 4. Проблемы хакерства.	Кванториум	Собеседование
5.				Практическая работа	1	Тема 5. Проблема краж персональных данных с помощью вредоносного ПО	Кванториум	Собеседование
6.				Практическая работа	1	Тема 6. Изучение структуры сообщества, авторов сообщений в социальной сети «ВКонтакте».	Кванториум	Практическая работа
7.				Теория	1	Тема 7. Правила функционирования сетевых сообществ. Правила сетевого общения.	Кванториум	Собеседование
8.				Практическая работа	1	Тема 8. Защищенность данных в сети. Проблемы утечки данных. Проблемы использования в сообщениях геотегов, столкновения с	Кванториум	Практическая работа

						неразумным и агрессивным поведением в сети.		
9.				Практическая работа	1	Тема 9. Благотворительность с помощью интернет. Риски потребительского поведения.	Кванториум	Практическая работа
10.				Теория Практическая работа	1	Тема 10. Проблема оказания поддельных услуг и распространения подозрительных объявлений об удаленной работе в социальных сетях.	Кванториум	Практическая работа
					10			

СОДЕРЖАНИЕ ПРОГРАММЫ

Тема 1. Информационная структура интернета, поисковые системы. Принципы эффективного поиска информации в интернете. Принципы оценки качества источников информации.

Теория. Информационная структура интернета, поисковые системы. Ознакомление с инструментом представления результатов работы в рамках курса, принципами подготовки эффективной презентации.

Постановка задачи групповой работы – эффективный поиск в интернете. Принципы эффективного поиска информации в интернете. Принципы оценки качества источников информации. Правила поиска в интернете.

Тема 2. Социальные сети и социальные медиа, поведение молодежи в сети, проблема лайков.

Теория. Социальные сети и социальные медиа, поведение молодежи в сети, проблема лайков. Элементы контента социальных сетей.

Тема 3. Фейковые сообщения и вредоносное ПО в сети Интернет.

Практика. Изучение фейковых сообщений и вредоносного ПО в сети Интернет и с помощью системы «Крибрум».

Тема 4. Проблема хакерства.

Теория. Рассмотрение наиболее крупных взломов системы и кибератак. Проблема хакерства.

Тема 5. Проблема краж персональных данных с помощью вредоносного ПО.

Теория. Проблема краж персональных данных с помощью вредоносного ПО.

Тема 6. Изучение структуры сообщества, авторов сообщений в социальной сети «ВКонтакте».

Практика. Понятие социальная группа, сообщество, субкультура, фэндом. Постановка задачи исследования. Изучение сообщений о сообществе в социальных сетях с помощью системы «Крибрум».

Тема 7. Правила функционирования сетевых сообществ. Правила сетевого общения.

Теория. Изучение правил функционирования сетевых сообществ. Правила сетевого общения.

Тема 8. Защищенность данных в сети. Проблемы утечки данных. Проблемы использования в сообщениях геотегов, столкновения с неразумным и агрессивным поведением в сети.

Теория. Защищенность данных в сети. Проблемы утечки данных. Действия при взломе аккаунтов. Безопасные пароли. Понятие персональных данных. Законодательство о защите персональных данных.

Риски нерационального и небезопасного использования личных и персональных данных в социальных сетях. Проблемы использования в сообщениях геотегов, столкновения с неразумным и агрессивным поведением в сети.

Тема 9. Благотворительность с помощью интернет. Риски потребительского поведения. Правила социальных сетей по размещению рекламы.

Практика. Исследование подозрительных объявлений о пожертвованиях в благотворительные фонды и частных сборах на лечение. Анализ объявлений о продаже в социальных сетях. Анализ с использованием системы «Крибрум» подозрительных объявлений о дарении, об акциях, розыгрышах призов и конкурсах репостов в социальных сетях.

Тема 10. Проблема оказания поддельных услуг и распространения подозрительных объявлений об удаленной работе в социальных сетях.

Практика. Анализ подозрительных сообщений, составление интеллектуальной карты действий при столкновении с подозрительным контентом.

Форма подведения итогов: публичное представление результатов исследований

СПИСОК ИСТОЧНИКОВ ИНФОРМАЦИИ

1. Ашманов И.С. Идеальный поиск в Интернете глазами пользователя. М.: Питер, 2011.
2. Богачева Т.Ю., Соболева А.Н., Соколова А.А. Риски интернет пространства для здоровья подростков и пути их минимизации // Наука для образования: Коллективная монография. М.: АНО «ЦНПРО», 2015.
3. Ефимова Л.Л., Кочерга С.А. Информационная безопасность детей: российский и зарубежный опыт: Монография. М.: ЮНИТИ-ДАНА, 2013.
4. Словарь молодежного и интернет-сленга / Авт.-сост. Н.В. Белов. Минск: Харвест, 2007.
5. Слугина Н. Активные пользователи социальных сетей Интернета. СПб.: Питер, 2013.
6. Солдатова Г., Зотова Е., Лебешева М., Вляпников В. Интернет: возможности, компетенции, безопасность. Методическое пособие для работников системы общего образования. Ч. 1. Лекции. М.: Google, 2013.
7. Солдатова Г., Рассказова М., Лебешева М., Зотова Е., Рогендорф П. Дети России онлайн. Результаты международного проекта EU Kids Online II в России. М.: Фонд Развития Интернет, 2013.
8. Солдатова Г.У., Рассказова Е.И., Зотова Е.Ю. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования. М.: Фонд Развития Интернет, 2013.
9. Солдатова Г.У., Шляпников В.Н., Журина М.А. Эволюция онлайн рисков: итоги пятилетней работы линии помощи «Дети онлайн» // Консультативная психология и психотерапия. 2015. № 3. С. 50-66.

Приложение

Оценочные материалы для итогового контроля

Тестовые задания для обучающихся 4-5 классов

Вопрос № 1: Как называется хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации.

Ответ: мошенничество

Вопрос № 2: Это русскоязычная зона всемирной сети Интернет**.**

Ответ: Рунет

Вопрос № 3: Кодекс правил поведения, общения в Сети, который соблюдает большинство пользователей**.**

Ответ: Сетикет

Вопрос № 4: Всемирная компьютерная сеть.

Ответ: Интернет

Вопрос № 5: Какая страна является родиной Интернета?

Ответ: США

Вопрос № 6: специальный компьютерный тест, проводимый для того, чтобы выяснить, кто пользователь — реальный человек или компьютер?

Ответ: Капча

Вопрос № 7: Информация, поступающая к нам от незнакомых людей или организаций, которым не было дано на это разрешение. Такая информация, как правило, поступает к нам по электронной почте

Ответ: Спам

Вопрос № 8: Специализированная программа для обнаружения компьютерных вирусов.

Ответ: Антивирус

Вопрос № 9: Персона, которая «взламывает» систему информационно-телекоммуникационную путем обхода или отключения мер по обеспечению безопасности

Ответ: Хакер

Вопрос № 10: Самый распространённый антивирус в России

Ответ: Касперский

Вопрос № 11: В какой стране появился Яндекс браузер

Ответ: России

Вопрос № 12: Чем опасны скачивать игры с пиратских сайтов

Ответ: Заражение

Вопрос № 13:

Верно ли, что социальные инженеры применяют психологические методы воздействия на людей через электронную почту, социальные сети и службы мгновенного обмена сообщениями?

Ответ: Верно

Вопрос № 14: Как называется сеть из заражённых устройств, расположенных по всему миру

Ответ: Ботнет

Тестовые задания для обучающихся 6-7 классов

Вопрос №1

Защита информации – это:

1. получение субъектом возможности ознакомления с информацией,в том числе при помощи технических средств
2. процесс сбора, накопления, обработки, хранения, распределения и поиска информации
3. деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию
4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям.

Вопрос№2

Доступ к информации — это:

1. возможность за приемлемое время получить требуемую информационную услугу
2. преобразование информации, в результате которого содержаниеинформации становится непонятным для субъекта, не имеющего доступа
3. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на нее
4. процесс сбора, накопления, обработки, хранения, распределения ипоиска информации

Вопрос №3

Защита информации от утечки — это деятельность по предотвращению:

1. деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количествополучателей информации
2. деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником либо владельцем информации прав или правил доступа к защищаемой информации
3. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами илисобственником, владельцем информации прав или правил доступа к защищаемой информации
4. деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа (НСД) к защищаемой информации и получения защищаемой информации злоумышленниками

Вопрос №4

Защита информации от несанкционированного доступа — это деятельность по предотвращению:

1. неконтролируемого распространения защищаемой информации отее разглашения, несанкционированного доступа (НСД) к защищаемой информации и получения защищаемой информации злоумышленниками

2. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами илисобственником, владельцем информации прав или правил доступа к защищаемой информации

3. деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником либо владельцем информации прав или правил доступа к защищаемой информации

4. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации

Вопрос №5

Защита информации от разглашения — это деятельность по предотвращению:

1. деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником либо владельцем информации прав или правил доступа к защищаемой информации

2. получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами илисобственником, владельцем информации прав или правил доступа к защищаемой информации

3. неконтролируемого распространения защищаемой информации отее разглашения, несанкционированного доступа (НСД) к защищаемой информации и получения защищаемой информации злоумышленниками

4. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

Вопрос №6

Собственник как субъект доступа к информации — это:

1. физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов

2. субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательнымиактами

3. субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации

Вопрос №7:

Носитель информации — это:

1. субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника, в соответствии с установленными правами и правилами доступа к информации либо с их нарушением

2. физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов

3. субъект, осуществляющий пользование информацией и реализующий

полномочия распоряжения в пределах прав, установленных законом и/или собственником информации

4. субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательнымиактами

5. участник правоотношений в информационных процессах

Вопрос №8

Укажите субъектов доступа к информации:

1. носитель
2. потребитель
3. накопитель
4. собственник
5. владелец

Вопрос №9

Потребитель информации имеет:

1. определенный договором или законом набор прав доступа кинформации
2. полный набор прав доступа к информации
3. ограниченный другими субъектами набор прав

Вопрос №10

Владелец информации — это:

1. субъект, пользующийся информацией, полученной от ее собственника или посредника, в соответствии с установленными правами и правилами доступа к информации либо с их нарушением

2. субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации

3. субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательнымиактами

Вопрос №11

Пользователь (потребитель) информации — это:

1. субъект, пользующийся информацией, полученной от ее собственника или посредника, в соответствии с установленными правами и правилами доступа к информации либо с их нарушением

2. субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации

3. субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательнымиактами

Вопрос №12

Потенциальная возможность неправомерного или случайного воздействия на объект защиты, приводящая к потере или разглашению информации:

1. атака
2. угроза
3. уязвимость

Вопрос №13

Целостность – это

1. защита от несанкционированного доступа к информации, свойство информации быть известной и доступной, только прошедшим проверку (авторизацию) субъектам системы (пользователям, программам, процессам)
2. актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения
3. возможность за приемлемое время получить требуемую информационную услугу

Вопрос №14

Вид источника угрозы ИБ, характер возникновения которогообусловлен действиями субъекта:

1. техногенный источник
2. антропогенный источник
3. стихийный источник

Вопрос №15

Источники угроз ИБ, определяемые технократической деятельностью человека и развитием цивилизации:

1. стихийный источник
2. антропогенный источник
3. техногенный источник

Вопрос №16

Системный администратор, работающий в штате вашей организации, относится к:

1. антропогенным источникам угроз ИБ
2. техногенным источникам угроз ИБ
3. внешним источникам угроз ИБ
4. внутренним источникам угроз ИБ

Вопрос №17

Степень квалификации и привлекательность совершения деяний со стороны источника угрозы (для антропогенных источников), или наличие необходимых условий (для техногенных и стихийных источников):

1. готовность источника

2. фатальность
3. возможность возникновения источника

Вопрос №18

Факторы, приводящие к нарушению безопасности информации наконкретном объекте информатизации:

1. угроза
2. окно опасности
3. уязвимость

Вопрос №19

Уязвимости, зависящие от действий сотрудников предприятия:

1. объективные
2. случайные
3. субъективные

Вопрос №20

Тип угроз ИБ, вызванных воздействием на компьютерную системуобъективных физических процессов или стихийных природных явлений:

1. Антропогенные
2. Стихийные
3. Естественные
4. Искусственные
5. Техногенные

Вопрос №21

Естественные угрозы безопасности информации вызваны:

1. ошибками при действиях персонала
2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения
3. воздействиями объективных физических процессов или стихийных природных явлений, не зависящих от человека
4. корыстными устремлениями злоумышленников

Вопрос №22

Нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях) относится к:

1. активным угрозам
2. непреднамеренным искусственным угрозам
3. преднамеренным искусственным угрозам
4. естественным угрозам

Вопрос №23

Угрозы ИБ, реализация которых не влечет за собой измененииструктуры данных (копирование):

1. естественные угрозы
2. пассивные угрозы
3. активные угрозы
4. искусственные угрозы

Вопрос №24

Угрозы ИБ, реализация которых меняет структуру и содержаниекомпьютерной системы (внедрение специальных программ):

1. искусственные угрозы
2. пассивные угрозы
3. активные угрозы
4. естественные угрозы

Вопрос №25

По размерам наносимого ущерба угрозы делятся на:

1. физические, программно-математические, организационные
2. общие, локальные, частные
3. пассивные и активные

Ответы

В1	**В 2**	**В 3**	**В 4**	**В 5**	**В 6**	**В 7**	**В 8**	**В 9**	**В 10**	**В 11**	**В 12**
3	1	4	3	4	2	2	2,4,5	3	3	1	2
В 13	**В 14**	**В 15**	**В 16**	**В 17**	**В 18**	**В 19**	**В 20**	**В 21**	**В 22**	**В 23**	**В 24**
2	2	3	1	1	3	3	3	3	3	2	3
В 25											
2											