Министерство образования и науки Астраханской области

Государственное бюджетное профессиональное образовательное учреждение Астраханской области «Астраханский колледж вычислительной техники»

Согласовано

Зам. директора по УМиВР

_____С.В.Расторгуева

«_5_»__декабря_____2023 г.

Утверждаю

Директор колледжа

_____Д.А.Лунев

«_5_»__декабря_____ 2023 г.

Программа

дополнительного образования

«Кибергигиена»

Астрахань

Аннотация программы дополнительного образования

Кибергигиена

Программа дополнительного образования разработана на основе:

Профессионального стандарта «Специалист по защите информации в автоматизированных системах» (утвержден приказом Минтруда России от от 14.09.2022 № 525н).

Программа дополнительного образования «Кибергигиена» может быть реализована с использование электронного обучения и дистанционных образовательных технологий.

Организация-разработчик:

Государственное бюджетное профессиональное образовательное учреждение Астраханской области «Астраханский колледж вычислительной техники» (ГБПОУ АО «АКВТ»).

Программу разработала

Староверова Е.Л., преподаватель дисциплин профессионального цикла ГБПОУ АО «АКВТ»

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Нормативно-правовую основу разработки образовательной программы дополнительного образования «Кибергигиена» составляют:

Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

Приказ Министерства образования и науки Российской Федерации от 23.08.2017 № 816 «Об утверждении порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»;

Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» (утвержден приказом Минтруда России от от 14.09.2022 № 525н).

К освоению дополнительных образовательной программы допускаются:

– учащиеся 7-9 классов, не имеющих специальной подготовки.

Документ, выдаваемый после завершения обучения: свидетельство.

2. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

2.1. Цель реализации программы

Программа «Кибергигиена» предназначена для слушателей, не имеющих образования и направлена на получение первичных навыков согласно плану курса, а также для дальнейшего развития умений и навыков в области информационной безопасности.

Программа также направлена на осознание учащимися роли кибербезопасности как перспективного направления развития IT-отрасли в Российской Федерации.

2.2. Планируемые результаты обучения

В результате освоения дисциплины обучающийся должен

уметь:

— осуществлять поиск достоверной информации в интернет-пространстве;

— работать с поисковыми системами, общедоступными средствами поиска информации в интернет-пространстве;

— выявлять признаки рискованного и опасного поведения и различных угроз в интернет-пространстве (фишинг, мошенничество, вовлечение в опасные виды деятельности), уметь идентифицировать их в социальных сетях;

— использовать антивирусное ПО для защиты от вредоносных программ;

— уметь создавать двухфакторную аутентификацию;

— свободно ориентироваться в интернет-пространстве, использовать различные типы источников для решения научно-исследовательских задач;

— ставить цели, планировать свою работу и следовать намеченному плану, критически оценивать достигнутые результаты;

— проектировать и создавать собственные проекты корпоративной защиты для обеспечения правил кибергигиены, создавать правила политики безопасности в DLP-системе;

— представлять результаты своей работы окружающим, распространять контент по кибергигиене в социальных сетях, аргументировать свою позицию;

— работать в соцсетях и мессенджерах по распространению правил кибергигиены, вести канал в роли администратора, фильтровать нежелательный контент;

— участвовать в профильных мероприятиях: конференции по информационной безопасности, социальных, благотворительных, волонтерских проектах Астраханской области, направленных на кибербезопасность

знать:

— правила безопасного поведения в интернет-пространстве, рационального использования персональных данных, защиты от вредоносных воздействий;

— типы злоумышленников, модель жертвы киберпреступлений;

— типы киберпреступлений, правила кибергигиены для каждого типа;

— типы источников информации и разновидности контента;

— современные требования в области информационной безопасности со стороны государства,

— функции Астраханского штаба кибербезопасности;

— функции, а также возможность принятия участия в волонтерском движении по кибербезопасности ГБПОУ АО «Астраханский колледж вычислительной техники»

— правила безопасной работы на компьютере.

личностные результаты развития:

— осознание себя гражданином и защитником великой страны

— активная гражданская позиция, демонстрирующая приверженность принципам честности, порядочности, открытости;

— активный и участвующий в территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций;

— демонстрирующий навыки анализа и интерпретации информации из различных источников с учетом нормативно-правовых норм;

— развитие внимания, памяти, восприятия, образного мышления;

— развитие логического и пространственного воображения;

— развитие творческих способностей и фантазии;

— развитие мотивации к познанию;

— формирование положительных черт характера: трудолюбия, аккуратности, собранности, усидчивости, отзывчивости, патриотизма;

— развитие мотивации к профессиональному самоопределению;

— сплочение семьи для решения общих позитивных задач на повышение уровня кибербезопасности.

2.3. Объем программы (трудоемкость)

Общая трудоемкость **72** академических часа.

2.4. Форма обучения

Форма обучения – очная. При наличии технических возможностей у слушателей программа может быть реализована полностью или частично с использованием электронного обучения и дистанционных образовательных технологий.

3. СОДЕРЖАНИЕ ПРОГРАММЫ

3.1. Учебный план и календарный учебный график

Учебный план

программы дополнительного образования

«Кибергигиена»

Категория слушателей: программа рассчитана на учащихся 7-9 классов, не имеющих специальной подготовки.

Срок обучения – 72 часа.

Форма обучения – очная с возможностью применения дистанционных технологий.

№ п/п	Название модуля, темы	Количество часов			Формы аттестации/контроля
		Всего	Теория	Практика	
1	Вводное занятие. Инструктаж по технике безопасности	**2**	2	-	
	Модуль 1 «Базовый»				
2	Введение в предмет. Кибербезопасность и кибергигиена в реальных условиях. Киберугрозы	**4**	2	2	Опрос, решение ситуационных задач
3	Киберпреступник и кибержертва	**4**	2	2	Викторина «Киберпреступник», викторина «Влюбить в профессию - Профессии будущего в сфере кибербезопасности»

4	Развитие кибергигиены как образа мышления	**8**	2	6	Решение ситуационных задач Создание чек-листа правил кибергигиены: уровень пользователя, продвинутый уровень Написание постов с правилами кибергигиены на Telegram канале по информационной безопасности «Союз БЕЗопасности» для распространения в сети Интернет, парная работа
5	Кибервымогатели — программное обеспечение киберпреступников	**2**	2	-	Опрос
6	Современные требования в области информационной безопасности со стороны государства. Кибервойска в Российской Федерации	**8**	4	4	Дискуссия «Какими должны быть кибервойска в России» Решение ситуационных задач
7	Деятельность штаба по обеспечению кибербезопасности на	**2**	2	-	Опрос

	территории Астраханской области, созданного губернатором Астраханской области И.Ю. Бабушкиным				
8	Деятельность отряда киберволонтеров «Киберпатруль» на базе ГБПОУ АО «Астраханский колледж вычислительной техники»	**6**	2	4	Круглый стол с приглашением эксперта «Личностные ресурсы для повышения киберграмотности граждан моей страны»
	Итого Модуль 1	**36**	**18**	**18**	
	Модуль 2 «Проектный»				
9	Интернет: стильный или стерильный? Безопасный поиск информации в сети	**6**	2	4	1 этап - Практическая работа «Поиск информации в сети Интернет» 2 этап- проведение дискуссии
10	Фейк. Фейковая информация в сети Интернет	**4**	2	2	Проверка достоверности фото и видео с помощью разных сервисов. Индивидуальная работа, групповая дискуссия
11	Персональные данные. Публикации в соцсетях.	**4**	2	2	Практическая работа

	Правила кибергигиены при работе в соцсетях и сообществах. Двухфакторная аутентификация				«Двухфакторная аутентификация в мессенджерах и соцсетях»
12	Вирусы. Правила кибергигиены для защиты от вирусов. Антивирусное программное обеспечение	**4**	2	2	Практическая работа «Установка и настройка антивирусного программного обеспечения» на виртуальной машине
13	Платежное мошенничество. Правила кибергигиены	**2**	2	-	Опрос
14	Кибербуллинг. Правила личной кибергигиены	**4**	2	2	Творческая работа. Семейный проект «Составление семейного календаря кибердел и кибердостижений»
15	Кибергигиена на рабочем месте. DLP-система как помощь в поддержке правил кибергигены для обеспечения корпоративной защиты	**6**	4	2	Практическая работа «Разработка правил безопасности в DLP-системе Infowatch для обеспечения работы правил

					кибергигиены в организации»
16	Итоговое занятие	**4**	-	4	Итоговая работа в формате игровой практики «Найди злоумышленника» (игровая механика игры Мафия)
	Итого Модуль 2	**34**	**16**	**20**	
Итого		**72**	**34**	**38**	

3.2. Рабочие программы модулей (курсов)

Модуль 1 «Базовый»

Введение в предмет. Кибербезопасность и кибергигиена в реальных условиях. Киберугрозы

Специалист по кибергигиене – профессия будущего. Кибербезопасность и кибергигиена в реальных условиях функционирования организаций. Роль кибергигиены в сфере жизнедеятельности человека.

Подмножество «Кибербезопасность» в множестве «Информационная безопасность»

Обзор актуальных киберугроз

Практическая часть:

Просмотр фрагментов документального сериала о киберугрозах в Российской Федерации «Невидимая война: что такое кибербезопасность», **разбор ситуационных задач** – публичная индивидуальная работа

Критерии оценки: Использование теоретических знаний из разных образовательных областей, обоснование ответа, правильность и полнота выполнения заданий, предложение нестандартного решения задачи

Киберпреступник и кибержертва

Модель кибернарушителя. Портрет киберпреступика и кибержертвы. Виды злоумышленников: белый, серый, черный хакер. Мотивы киберпреступлений. Типы викитимного поведения, способы предупреждения реализации киберугроз

Практическая часть:

Викторина «Киберпреступник» Командная работа

Викторина «Влюбить в профессию - Профессии будущего в сфере кибербезопасности» Командная работа

Критерии оценки: Работа в команде, Соблюдение регламента и этапов в работе, степень ответственности в личной зоне задач, личный вклад в работу команды, аргументация ответов (ответы на вопросы преподавателя/личная инициатива)

Развитие кибергигиены как образа мышления

Обзор правил кибергигиены. Составление таблицы соответствия правил кибергигиены и личной гигиены. Способы внедрения правил кибергигиены в повседневную жизнь

Практическая часть:

1. Просмотр фрагментов документального сериала о киберугрозах в Российской Федерации «Невидимая война: кто такие хакеры», разбор ситуационных задач - публичная индивидуальная работа

Критерии оценки: Использование теоретических знаний из разных образовательных областей, обоснование ответа, правильность и полнота выполнения заданий, предложение нестандартного решения задачи

2. Создание чек-листа правил кибергигиены: уровень пользователя, продвинутый уровень. Создание индивидуального чек-листа используемых правил кибергигиены по образцу (два уровня сложности), индивидуальная работа

Критерии оценки: дизайн, лаконичность и доступность информации для граждан разных возрастных категорий, возможность выполнения правил или внедрения в реальную жизнь, время создания, актуальность информации

3. Написание постов с правилами кибергигиены на Telegram канале по информационной безопасности «Союз БЕЗопасности» для распространения в сети Интернет, работа по заранее распределенным темам: Своевременная очистка жесткого диска, Антивирусное программное обеспечение, Правила использования лицензионного программного обеспечения, Парольная защита, Брандмауэры (t.me/souzBEZopasnosti). Развитие навыков администрирования и модерации телеграмм-канала. Ведение

тематических сообществ в социальных сетях, создание и распространение полезного позитивного контента по тематике. Работа в парах

Критерии оценки: достоверность и актуальность, использование официальных источников информации, наличие картинок по теме поста, дизайн, доступность для понимания различными категориями граждан, количество просмотров и существенных комментариев к посту, распределение работы в паре

Кибервымогатели — программное обеспечение киберпреступников

Шантаж в сети Интернет. Программы-блокировщики с требованием выкупа. Вредоносные программы-шифровальщики.

Современные требования в области информационной безопасности со стороны государства. Кибервойска в Российской Федерации

Рыцари программного кода — Кибервойска в России: современное предложение руководителя Минцифры Максуда Шадаева. Проблемы, варианты развития, задачи кибервойск

Практическая часть:

1. **Дискуссия** «Какими должны быть кибервойска в России»

Причины и целесообразность создания кибервойск как отдельной структуры. Какими качествами должен обладать сотрудник кибервойск – групповая работа

Критерии оценки: Четкая формулировка тезисов, грамотность высказываний, патриотическая направленность, уважительное отношение к членам дискуссии, соблюдение временного регламента, обоснование точки зрения, креативность, умение поставить уточняющий вопрос, позволяющий продвигать дискуссию вперед, соблюдение этических норм ведения дискуссии

2. Просмотр фрагментов документального сериала о киберугрозах в Российской Федерации «Методы работы киберпреступников и киберзащитников», **разбор ситуационных задач -** публичная индивидуальная работа

Критерии оценки: Использование теоретических знаний из разных образовательных областей, обоснование ответа, правильность и полнота выполнения заданий, предложение нестандартного решения задачи

Деятельность штаба по обеспечению кибербезопасности на территории Астраханской области, созданного губернатором Астраханской области И.Ю. Бабушкиным

Роль, состав и функции штаба по обеспечению кибербезопасности на территории Астраханской области

Выявление источников внутренних и внешних угроз кибербезопасности, определение приоритетных направлений деятельности в данной сфере

Деятельность отряда киберволонтеров «Киберпатруль» на базе ГБПОУ АО «Астраханский колледж вычислительной техники»

Добровольческая (волонтерская) деятельность. Деятельность отряда киберволонтеров «Киберпатруль» на базе ГБПОУ АО «Астраханский колледж вычислительной техники». Сложившаяся ситуация в мире, Российской Федерации и непосредственно в Астраханской области. Кибердружины и киберотряды, создающиеся на базе образовательных организаций (школ, техникумов, колледжей или университетов). Повышение качества и эффективности просветительских, профилактических и образовательных мероприятий, направленных на противодействие идеологии терроризма и проявлений экстремизма в образовательной среде и сети Интернет.

Практическая часть:

Круглый стол с приглашением эксперта «Личностные ресурсы для повышения киберграмотности граждан моей страны», групповая работа, возможны выступления с предложениями

Модуль 2. Проектный

Интернет: стильный или стерильный?

Безопасный поиск информации в сети. Переходы по ссылкам результатов поиска. Причины перехода по «первой ссылке». Модель поведения «Любовь с первого взгляда». Модель поведения «Хороший отказ». Знаки Яндекса —специальные метки для удобного поиска. Правила анализа результатов поиска в Интернет

Практическая часть:

1 этап - Практическая работа «Поиск информации в сети Интернет». Индивидуальная работа по карточкам по вариантам. 2 этап- проведение дискуссии на анализ достоверности найденной информации

Критерии оценки: Находить официальный источник, авторов (формировать список литературы), искать сомнительные мелочи, сравнивать информацию в разных источниках, обращать внимание на дату выхода информации, обоснованно спорить, дискутировать

Фейк. Фейковая информация в сети Интернет

Что такое фейковая информация. Исторические корни фейка. Типы фейков, время жизни фейка. Отличительные особенности фейков: какие эмоции вызывают. Точка боли. Действия при обнаружении фейка, сохранение критического мышления. Куда пожаловаться на фейк. Виды ответственности перед законом РФ за распространение фейковой информации.

Практическая часть:

Проверьте достоверность фото и видео с помощью разных сервисов. Индивидуальная работа, групповая дискуссия.

Tineye — для поиска первоисточника фото

Чтобы проверить, является ли видео новым, воспользуйтесь сервисом Youtube Data Viewer — он поможет найти подобные ролики и сам первоисточник.

Есть инструмент Metadata2go, позволяющий определить дату съемки, геолокацию, устройство. Но важно помнить — метаданные также могут быть искажены либо из-за сброса настроек на компьютере, либо намеренно.

Если хотите проверить материал на использование DeepFake — технологии синтеза изображения, основанной на искусственном интеллекте, которую используют для соединения и наложения существующих изображений и видео на исходники — обратитесь к сервису Scanner.deepware.

Сайты проверки фактов:

- Snopes
- PolitiFact
- Fact Check
- BBC Reality Check
- «Проверено» — русскоязычное издание, которое позаимствовало рейтинговую систему Snopes. «Проверено» разбирает факты на разные темы — здесь есть и международная повестка, и чисто российская. Правда, в отличие от Snopes, «Проверено» почти не занимается проверкой информации, связанной с политикой.
- Fakecheck — российское интернет-издание. Fakecheck занимается проверкой фактов из российской повестки. Его рейтинговая система называется «фейкометр» и содержит восемь оценок. Помимо стандартных, таких как «Правда», «Fake!» и градаций между ними,

есть также три отдельные категории. Это «Осторожно» и «Без оценки», которые означают, что информация изначально поступила из закрытого или анонимного источника и ее пока невозможно проверить, а также «Сатирикон» — категория новостей, которые не скрывают свою сатирическую натуру.

Критерии оценки: критическое мышление, представление ресурса, проверка фактов, оценка комментариев, оценка собственных убеждений, не является ли статья шуточной, первоисточник, поиск информации в других источниках, выделение особенностей текста, проверка достоверности фото и видео

Персональные данные. Публикации в соцсетях. Правила кибергигиены при работе в соцсетях и сообществах. Двухфакторная аутентификация

Что является персональными данными. Категории персональных данных. 152 ФЗ «О защите персональных данных», требования. Правила кибергигиены при работе в соцсетях и сообществах: правила личных переписок, комментарии, выкладка постов, геолокация. Двухфакторная аутентификация в операционной системе, мессенджере, браузере, социальной сети или игре. Генератор паролей, вход по смс, отпечаток пальца: достоинства и недостатки.

Практическая часть:

Практическая работа «Двухфакторная аутентификация в мессенджерах и соцсетях». Включение двухфакторной аутентификации на личных страницах в сервисах ВКонтакте и Telegram, индивидуальная работа

Критерии оценки: обоснование выбора способов двухфакторной аутентификации, знать типы идентификационных данных, представление способов восстановление доступа к аккаунту, выбор методов реагирования при взломе страницы, умение обращаться со службами поддержки

Вирусы. Правила кибергигиены для защиты от вирусов. Антивирусное программное обеспечение

Основные пути проникновения вирусов в компьютер, Сетевые, файловые, загрузочные, файлово-загрузочые, системные, резидентные, нерезидентные , безвредные, неопасные, опасные, очень опасные, вирусы-«спутники», простейшие вирусы, Ретро-вирусы, репликаторные, вирусы-«черви», «паразитические», «студенческие», «стелс»-вирусы (невидимки), вирусы-призраки, макровирусы, квазивирусные, или «троянские», логические бомбы, мутанты. Признаки заражения. Антивирусные программы, отечественное продукты, обновление антивирусных баз

Практическая часть:

Практическая работа «Установка и настройка антивирусного программного обеспечения» на виртуальной машине, работа в парах

Критерии оценки: обоснование выбора антивирусного программного продукта, понимание механизмов защиты, умение сравнивать с аналогами, умение подбора версии продукта в соответствии с задачей, успешная установка продукта на виртуальную машину, обновление антивирусных баз

Платежное мошенничество. Правила кибергигиены

Мошенничество в сфере электронных платежей. Мошенничество в Интернет-магазинах. Телефонные мошенничества. Мошенничество с пластиковыми картами. Мошенничество с банковскими картами. Фишинг. Спуфинг, сайты-близнецы. Техника безопасности при оплате картой в сети Интернет. Ответственность мошенников

Кибербуллинг. Правила личной кибергигиены

Реальное и виртуальное «быкование», разница и сходства методов. Модель злоумышленника, мотивы, ответственность. Клевета, флейминг, нападки. Агрессор, жертва, наблюдатель – роли участников кибербуллинга. Методы поддержки жертвы, профилактические меры, меры помощи близким (одноклассникам, друзьям). Как не стать жертвой кибербуллинга. Меры профилактики от роли агрессора. Действия, если оказался наблюдателем.

Практическая часть:

Составление семейного календаря кибердел и кибердостижений. Творческая работа. Семейный проект. Социально-волонтёрский проект по духовно-нравственному воспитанию и формированию семейных ценностей, обучению правилам кибергигиены членов семьи, друзей.

По заранее подготовленным шаблонам календаря кибердел и кибердостижений ученикам предстоит заполнить его дома в электронном виде, записав используемые в семье правила и кибергигиены, а также о помощи в области кибергигиены ближним (установил антивирус, создал бабушке аккаунт в соцсетях с надежным паролем, научил родителей правильно реагировать на звонки посторонних, научил безопасно использовать платежные системы и данные банковских карт, вовремя удалять неиспользуемый контент с компьютера и личного телефона и т.д.)

Выкладка готового материала: посты с правилами кибергигиены, используемыми семьей в течение 3 дней на Telegram канале по информационной безопасности «Союз БЕЗопасности» для распространения в сети Интернет (t.me/souzBEZopasnosti)

Критерии оценки: количество охваченных людей для помощи (членов семьи, друзей), разнообразие и количество используемых правил кибергигиены, подписка на канал «Союз БЕЗопасности» (t.me/souzBEZopasnosti) и чтение полезного контента, участие в обсуждении правил кибергигены, отзывы о календарях кибергигены сверстников, оформление семейного календаря

Кибергигиена на рабочем месте. DLP-система как помощь в поддержке правил кибергигены для обеспечения корпоративной защиты

Уязвимости конфиденциальной информации на рабочем месте. Корпоративная защита. Правила кибергигиены для сохранения защиты информационных ресурсов компании от внутренних утечек и хакерства. DLP-система уровня пользователя, обзор, функции. DLP- система от Infowatch, интерфейс, правила работы, демонстрация возможностей для поддержания правил кибергигиены. Разработка правил в DLP- системе от Infowatch, проверка работоспособности

Практическая часть:

Практическая работа «Разработка правил безопасности в DLP-системе Infowatch для обеспечения работы правил кибергигиены в организации». Индивидуальная работа. Работа в виртуальных машинах. Проверка работоспособности. Работа с перехватчиками: Application Monitor. Позволяет контролировать доступ сотрудников к приложениям при помощи черных и белых списков.

Clipboard Monitor. Позволяет контролировать вставку данных из буфера обмена. Система позволяет запрещать вставку данных в приложения из списка либо все операции вставки данных в приложения терминальной сессии.

Cloud Storage Monitor. Позволяет контролировать веб-клиенты облачных хранилищ.

File Monitor. Позволяет отслеживать следующие действия с файлами на съемных и сетевых ресурсах: о копирование файла на сетевые ресурсы

HTTP(S) Monitor. Позволяет контролировать обмен данными по протоколам HTTP и HTTPS.

IM Client Monitor. Позволяет контролировать доступ сотрудников к клиентам мгновенного обмена сообщениями и протоколам передачи данных: Skype, WhatsApp, Viber, Telegram, XMPP, MMP, Facebook, Vkontakte.

Mail Monitor. Позволяет контролировать отправку и получение электронной почты.

Photo Monitor. Позволяет создавать теневые копии фотографий, сделанных при помощи камер мобильных устройств.

Критерии оценки: Создана агентская политика, есть скриншот(ы), подтверждающие создание и срабатывание, проверка работоспособности правила, верное реагирование правила при проверке, нет ложных срабатываний, верно выбран перехватчик

Итоговая аттестация

Итоговая работа в формате игровой практики «Найди злоумышленника» (игровая механика игры Мафия)

Игра «Злоумышленник» (игровая механика игры Мафия)

2 команды по 5 человек. Карточки заранее будут разложены тыльной стороной на столах, чтоб не создавать суету и не тратить время на их раздачу. Ребята поднимают карточки, смотрят свою роль, не говоря никому

1я команда – Отдел информационной безопасности МБОУ СОШ№8 **(пример)**

2я команда - Отдел информационной безопасности Стационар №1 (больница) **(пример)**

В каждой команде есть роли:

Администратор отдела 1 чел- Несет ответственность за работу всего отдела и принимает итоговые решения

Сотрудники отдела 4 чел- Защищают важную и ценную информацию компании, подчиняются администратору безопасности и выполняют его поручения.

Среди 4-х сотрудников одному попадается карточка злоумышленника. Это сотрудник, как и все, но выдавать себя нельзя. Злоумышленники есть 2х типов (см карточки) для создания реальных вариантов функционирования организаций.

Злоумышленники незаметно создают ситуации совершения кражи информации, мешают работе отдела, удаляют документы, дают вредные советы

Публично открывается только одна роль – администратор, так как он раздает задания и принимает итоговые решения.

Ход игры:

Сотрудники переходят в «отделы информационной безопасности» (рассаживаются за компьютеры группами - школа и больница)

Ситуация: при обработке конфиденциальных данных в школе (совещание с родителями ученика, обсуждение состояния здоровья учеников и сотрудников, психологического климата, деструктивного поведения, хранение документов на компьютере) и больнице (консилиум с обсуждением диагнозов и методов лечения, новых технологий, персональных данных пациентов, хранение документов на компьютере), вероятны случаи передачи конфиденциальной информации злоумышленникам ввиду несоблюдения правил личной и корпоративной кибергигиены, в результате чего возможны последствия: шантаж, неправомерное вымогательство средств, вмешательство в личную

жизнь; угрозы детям, пациентам и сотрудникам, например, в случае публикации в соцсетях.

Организации, в свою очередь, допустившие утечку персональных данных, понесут ответственность:

• гражданскую, в виде взыскания в судебном порядке понесенных гражданами убытков и морального вреда;

• административную, в виде наложения штрафа, приостановления или запрета деятельности, связанной с обработкой персональных данных;

• уголовную, в случае неправомерного распространения ПДн, причинившего существенный ущерб и передаче информации в правоохранительные органы.

Преподаватель выступает в роли консультанта по вопросам защиты

Задания (по 30 минут):

Задача 1 - Документационная

Выбрать 2 документа, необходимых для подкрепления правил информационной безопасности для ознакомления сотрудников с ограничениями (будет 5 документов на компьютере, следует выбрать 2 необходимых и распечатать их)

Результат:

Распечатанные документы с подписью администратора – 2 документа

Задача 2 - Технологическая

Выявить злоумышленника среди сотрудников компании. Проводить анализ деятельности каждого участника, определить какие правила кибергигиены не соблюдают сотрудники

Результат:

Обоснованный выбор злоумышленника

Итог:

После выполнения заданий команды возвращаются за общий стол и представляют результаты (10 минут на команду). Во время представления результатов вторая команда внимательно слушает (и наоборот) для составления выводов о том, какие общие цели есть у всех организаций, от кого и от чего нужно защищаться, какие правила кибергигиены были нарушены и какие следует ввести. Выясняется, верно ли был обнаружен злоумышленник среди сотрудников

Критерии оценки для командного зачета:

Выясняется, верно ли был обнаружен злоумышленник среди сотрудников, по каким критериям, выявлены ли были средства хищения информации, выводы, что сотрудники могут вести себя по-разному, на что следует обращать внимание, призыв к порядочности, честности, патриотизму, роли каждого из нас в сфере защиты информации.

Критерии оценки для личного зачета:

- Работа в команде отдела безопасности
- Соблюдение регламента и аккуратность в работе
- Степень ответственности в личной зоне задач
- Личный вклад в работу отдела
- Работа на занятии (ответы на вопросы преподавателя/личная инициатива)

Сотрудник отдела информационной безопасности

Ты специалист, который стоит на страже интересов организации. Защищаешь важную и ценную информацию компании, подчиняешься администратору безопасности и выполняешь его поручения.

Несешь ответственность за защиту данных

Администратор отдела информационной безопасности

Ты специалист, осуществляющий контроль за обеспечением защиты информации всей организации.

Несешь ответственность за работу всего отдела и принимаешь итоговые решения

4. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

4.1. Материально-технические условия реализации программы

Для обучения слушателей программы используется оборудование мастерской IT-куба «Кибергигиена и работа с большими данными»:

- интерактивная доска;
- ноутбук;
- подключение к Интернет.

Программное обеспечение:

- операционная система Linux;
- офисный пакет;
- графический редактор;
- продукт виртуализации VMware Workstation;
- виртуальные машины: доменный сервер Demo.lab, IWDM сервер, IWDM клиент;
- свободно распространяемое антивирусное программное обеспечение;
- DLP-система Infowatch.

4.2. Учебно-методическое и информационное обеспечение.

Для педагога:

1. Ашманов И.С. Идеальный поиск в Интернете глазами пользователя. М.: Питер, 2011.

2. Ашманов И.С., Иванов А.А. Продвижение сайта в поисковых системах. М.: Вильямс, 2007.

4. Бек У. Общество риска. На пути к другому модерну. М.: Прогресс Традиция, 2000.

7. 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.

10. Волков Б.С., Волкова Н.В., Губанов А.В. Методология и методы психологического исследования: Учебное пособие. М.: Академический проект; Фонд «Мир», 2010.

11. Гаврилов К.В. Как сделать сюжет новостей и стать медиатворцом. М: Амфора. 2007.

14. Горошко Е.И. Современная Интернет-коммуникация: структура и основные параметры // Интернет-коммуникация как новая речевая формация: коллективная монография / науч. ред. Т. Н. Колокольцева, О.В. Лутовинова. М.: Флинта: Наука, 2012.

16. Ефимова Л.Л., Кочерга С.А. Информационная безопасность детей: российский и зарубежный опыт: Монография. М.: ЮНИТИ-ДАНА, 2013.

21. Крупник А.Б. Поиск в Интернете: самоучитель. СПБ.: Питер, 2004.

22. Лукина М.М. Интернет-СМИ: Теория и практика. М.: Аспект-Пресс. 2010.

23. Машкова С. Г. Интернет-журналистика: учебное пособие. Тамбов: Издво ТГТУ, 2006.

27. Прохоров А. Интернет: как это работает. СПб.: БХВ - Санкт-Петербург, 2004.

28. Рубинштейн С. Л. Основы общей психологии. СПб.: Издательство «Питер», 2000.

29. Словарь молодежного и интернет-сленга / Авт.-сост. Н.В. Белов. Минск: Харвест, 2007.

30. Слугина Н. Активные пользователи социальных сетей Интернета. СПб.: Питер, 2013.

31. 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.

33. Солдатова Г.У., Рассказова Е.И., Зотова Е.Ю. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования. М.: Фонд Развития Интернет, 2013.

36. Федоров А.В. Медиаобразование: вчера и сегодня. М: МОО ВПП ЮНЕСКО «Информация для всех», 2009.

37. Чернец В., Базлова Т. Иванова Э., Крыгина Н. Влияние через социальные сети. М.: Фонд «ФОКУС-МЕДИА», 2010.

40. Щербаков А.Ю. Интернет-аналитика. Поиск и оценка информации в web-ресурсах. Практическое пособие. М.: Книжный мир, 2012.

Для обучающихся:

1. Новые медиа. Социальная теория и методология исследований. Словарь-справочник. СПб.:Алетейя, 2016.

2.Эрик Куалман. Безопасная Сеть. Правила сохранения репутации в эпоху социальных медиа и тотальной публичности. Альпина Паблишер, 2017.

Электронные ресурсы нормативно-правового обеспечения:

1. https://www.garant.ru/ - правовая система «Гарант»
2. https://fstec.ru/ - сайт Федеральной службы по техническому и экспортному контролю
3. http://www.fsb.ru/ - сайт Федеральной службы безопасности Российской Федерации

4.3. Кадровое обеспечение программы

Количество лиц, привлеченных для реализации программы 1 чел. Из них:
- Экспертов с правом проведения чемпионата по соответствующей компетенции 1 чел.

№ п/п	ФИО	Статус в экспертном сообществе с указанием компетенции	Должность, наименование организации
1	Староверова Елена Львовна	Эксперт с правом проведения чемпионата по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»	Преподаватель ГБПОУ АО «Астраханский колледж вычислительной техники»