

Выписка из основной образовательной программы
среднего общего образования МАОУ Гимназия № 10
(приказ от 29.08.2023 № 70/03-од)

РАБОЧАЯ ПРОГРАММА

учебного курса «Киберугрозы финансовой отрасли»

для обучающихся 11 класса

1. Пояснительная записка

Целью настоящей программы учебного курса «Киберугрозы финансовой сферы» для 11 класса является ознакомление обучающихся с теоретическими и практическими аспектами в области кибербезопасности финансовой сферы.

Основные задачи изучения курса:

- 1) ознакомление с ключевыми видами киберугроз в финансовой сфере;
- 2) приобретение практических навыков распознавания киберугроз в финансовой сфере;
- 3) приобретение практических навыков ответственного цифрового поведения в условиях цифровой трансформации экономики: формирование культуры цифровой устойчивости и личной ответственности за безопасность персональных и финансовых данных, включая развитие навыков цифровой гигиены.

2. Планируемые результаты освоения учебного курса «Киберугрозы финансовой сферы»

Личностные результаты

в сфере гражданского воспитания: осознание ответственности за собственную цифровую безопасность как неотъемлемой части финансовой безопасности личности и общества; формирование активной гражданской позиции, основанной на понимании рисков цифровой среды и готовности противодействовать киберпреступности; уважение правопорядка и законодательства в области защиты персональных данных и финансовой информации;

в сфере патриотического воспитания: понимание значимости национальной киберсуверенности и устойчивости финансовой системы России; гордость за достижения отечественных разработок в области кибербезопасности; осознание своей роли в защите цифрового пространства своей страны;

в сфере духовно-нравственного воспитания: понимание недопустимости мошенничества и нарушения приватности других пользователей; готовность к солидарным действиям по предупреждению киберугроз в своем окружении; осознание «цифрового следа» и ответственного отношения к ресурсам информационной среды; понимание, что устойчивое цифровое будущее требует не только технической, но и этической устойчивости;

в сфере трудового воспитания: проявление интереса к современным и перспективным профессиям в сфере кибербезопасности и защиты финансовых данных; готовность к непрерывному самообразованию в быстро меняющейся технологической среде.

Метапредметные результаты

В сфере универсальных учебных познавательных действий:

владение базовыми логическими действиями: формулировать проблему, вопрос, требующий решения; устанавливать существенный признак или основания для сравнения, классификации и обобщения; определять цели деятельности, задавать параметры и критерии их достижения; выявлять закономерные черты и противоречия в рассматриваемых явлениях; разрабатывать план решения проблемы с учетом анализа имеющихся ресурсов; вносить коррективы в деятельность, оценивать соответствие результатов целям;

владение базовыми исследовательскими действиями: определять познавательную задачу; намечать путь ее решения и осуществлять подбор исторического материала, объекта; владеть навыками учебно-исследовательской и проектной деятельности; осуществлять анализ объекта; систематизировать и обобщать факты (в том числе в форме таблиц, схем); выявлять характерные признаки явлений в области финансов; раскрывать причинно-следственные связи событий прошлого и настоящего; сравнивать события, ситуации, определяя основания для сравнения, выявляя общие черты и различия; формулировать и обосновывать выводы; определять новизну и обоснованность полученного результата; представлять результаты своей деятельности в различных формах (сообщение, эссе, презентация, реферат, учебный проект и др.); объяснять сферу применения и значение проведенного учебного исследования в современном общественном контексте;

работа с информацией: осуществлять анализ учебной и внеучебной исторической информации (учебники, источники финансовой информации, в том числе научные публикации, научно-популярная литература, интернет-ресурсы и др.) – извлекать, сопоставлять, систематизировать и интерпретировать информацию; различать виды источников финансовой информации; высказывать суждение о достоверности и значении информации источника (по предложенным или самостоятельно сформулированным критериям); рассматривать комплексы источников, выявляя совпадения и различия их свидетельств; использовать средства современных информационных и коммуникационных технологий с соблюдением правовых и этических норм, требований информационной безопасности; создавать тексты в различных форматах с учетом назначения информации и целевой аудитории, выбирая оптимальную форму представления и визуализации.

В сфере универсальных коммуникативных действий:

общение: представлять особенности взаимодействия людей в области финансов в современном мире; участвовать в обсуждении событий и личностей прошлого и современности, выявляя сходство и различие

высказываемых оценок; излагать и аргументировать свою точку зрения в устном высказывании, письменном тексте; владеть способами общения и конструктивного взаимодействия, в том числе межкультурного, в школе и социальном окружении; аргументированно вести диалог, уметь смягчать конфликтные ситуации;

осуществление совместной деятельности: осознавать на основе исторических примеров значение совместной деятельности людей как эффективного средства достижения поставленных целей; планировать и осуществлять совместную работу, коллективные учебные проекты по экономике и финансам, в том числе на региональном материале; определять свое участие в общей работе и координировать свои действия с другими членами команды; проявлять творчество и инициативу в индивидуальной и командной работе; оценивать полученные результаты и свой вклад в общую работу.

В сфере универсальных регулятивных действий:

владение приемами самоорганизации своей учебной и общественной работы – выявлять проблему, задачи, требующие решения; составлять план действий, определять способ решения, последовательно реализовывать намеченный план действий и др.;

владение приемами самоконтроля – осуществлять самоконтроль, рефлекссию и самооценку полученных результатов; вносить коррективы в свою работу с учетом установленных ошибок, возникших трудностей;

принятие себя и других – осознавать свои достижения и слабые стороны в учении, школьном и внешкольном общении, сотрудничестве со сверстниками и людьми старших поколений; принимать мотивы и аргументы других при анализе результатов деятельности; признавать свое право и право других на ошибку; вносить конструктивные предложения для совместного решения учебных задач, проблем.

Предметные результаты

- знать и понимать сущность основных киберугроз финансовой сферы, включая методы социальной инженерии, фишинг, вредоносное ПО и атаки через цепочки поставок;
- владеть знаниями об архитектурных рисках современных финансовых технологий, таких как open banking (API) и экосистема Web3 (криптоактивы, смарт-контракты);
- понимать принципы работы и риски компрометации биометрических систем идентификации;
- уметь применять на практике правила цифровой гигиены для защиты персональных данных и финансовых активов при использовании

мобильных устройств, онлайн-платежей и банковских сервисов;

– быть способным разрабатывать и представлять эффективные информационно-просветительские материалы по вопросам кибербезопасности для своей целевой аудитории.

3. Содержание учебного курса «Киберугрозы финансовой сферы» 11 класс

Актуальные киберугрозы, направленные на финансовую инфраструктуру. Механизмы социальной инженерии и фишинга — включая дипфейки и QR-мошенничество — и способы их распознавания. Типы вредоносного ПО: стилеры, шифровальщики и банковские трояны, их воздействие на данные и активы. Уязвимости цепочек поставок и облачных сервисов, где ошибки конфигурации становятся вектором атак. Риски API в open banking и угрозы в экосистеме Web3: фишинг кошельков, утечки смарт-контрактов. Угрозы биометрическим данным и критическая роль цифровой гигиены: безопасность мобильных устройств, двухфакторная аутентификация, управление разрешениями.

4. Тематическое планирование с указанием количества часов, отводимых на освоение каждой темы, в том числе с учетом рабочей программы воспитания

11 класс

№ п/п	Тема	Кол-во часов	Деятельность учителя с учетом рабочей программы воспитания
1	Актуальность киберугроз финансовой сферы	2	устанавливать доверительные отношения между учителем и обучающимися, способствующих позитивному восприятию учащимися требований и просьб учителя побуждать обучающихся соблюдать на уроке принципы учебной дисциплины и самоорганизации использовать воспитательные возможности содержания учебного предмета через подбор соответствующих
2	Методологии социальной инженерии и фишинговых атак: когнитивные уязвимости и тактики манипуляции	2	
3	Технологические векторы атак: классификация вредоносного программного обеспечения	2	
4	Цепочки поставок как критическая уязвимость: анализ атак через сторонние сервисы и программные компоненты	2	
5	Уязвимости облачных инфраструктур и конфигурационные ошибки как вектор компрометации финансовых данных	2	
6	Архитектура API в open banking:	2	

	риски интерфейсов взаимодействия и механизмы защиты транзакций		текстов для чтения, задач для решения, проблемных ситуаций для обсуждения в классе
7	Киберугрозы в экосистеме Web3 и криптографических активов: от смарт-контрактов до фишинга кошельков	2	привлекать внимание обучающихся к обсуждаемой на уроке информации, активизации познавательной деятельности обучающихся
8	Биометрические системы как объект кибератак: риски компрометации персональных биоданных	2	
9	Цифровая гигиена как основа персональной киберустойчивости: безопасность мобильных устройств и сетевых сред	2	инициировать обучающихся к обсуждению, высказыванию своего мнения, выработке своего отношения по поводу получаемой на уроке социально значимой информации
10	Методы кибербезопасности в повседневной финансовой деятельности: от онлайн-платежей до мобильного банкинга	2	
11	Интеллектуальный кибер-квест: комплексная диагностика угроз в симулированной финансовой среде	2	применять на уроке интерактивные формы работы с обучающимися:
12	Деловая игра «Финансовая устойчивость организации»: управление киберрисками в условиях ограниченных ресурсов	2	групповая работа или работа в парах, которые учат обучающихся командной работе и взаимодействию с другими обучающимися
13	Встреча с экспертом: государственные и отраслевые подходы к противодействию киберугрозам в финансовом секторе	2	
14	Проектная деятельность: разработка информационно-просветительской кампании по кибербезопасности для сверстников	2	
15	Презентация проектов и оценка эффективности образовательных кампаний	2	
16	Рефлексия и метапознание: формирование личной модели цифровой устойчивости	2	
17	Итоговая церемония: вручение сертификата «Кибер-защитник финансовой сферы» и подведение итогов курса	2	
	Всего	34 ч.	