Приложение № 38
к приказу
от 21.06.2024 №30/1-h

ПРИНЯТО на заседании кафедры информатики ФМШ СФУ Протокол № 8 от «03» 06 2024г	ПРИНЯТО на заседании Ученого совета ФМШ СФУ Протокол № 7 от «06» 06 2024г.	УТВЕРЖДЕНО ДиректорФМШ СФУ _____ Е.А. Енгуразова «21» июня 2024 г.

РАБОЧАЯ ПРОГРАММА
СРЕДНЕГО ОБЩЕГО ОБРАЗОВАНИЯ
ЭЛЕКТИВНОГО КУРСА
«ВВЕДЕНИЕ В КИБЕРБЕЗОПАСНОСТЬ»

Составители:

Вайнштейн В.И., канд. физ.-мат. наук, заведующий кафедрой информационной безопасности Института космических и информационных технологий СФУ

Рачкин А.С., сотрудник кафедры информационной безопасности Института космических и информационных технологий СФУ

Красноярск 2024

Настоящая рабочая программа разработана на основе Федеральной образовательной программы среднего общего образования, в соответствии с требованиями Федерального государственного образовательного стандарта среднего общего образования и на основе требований к результатам освоения основной образовательной программы среднего общего образования физико-математической школы-интерната ФГАОУ ВО «Сибирский федеральный университет». В соответствии с учебным планом ФМШ СФУ элективный курс «Введение в кибербезопасность» изучается по выбору обучающихся 10 класса, в объеме 1 часа в неделю, 34 часа в год.

Курс «Введение в кибербезопасность» рассчитан на учащихся 10 класса профильной школы и направлен на углубление, совершенствование и систематизацию знаний и умений, освоенных в рамках общеобразовательного предмета «Информатика». В рамках курса рассматриваются основы информационной безопасности, способы решения задачи кибербезопасности.

Целесообразным является поддержка курса занятиями в модуле «Введение в кибербезопасность» программы дополнительного образования «Киберполигон и CTF».

Цели курса «Введение в кибербезопасность»: формирование у школьников представлений о современном уровне научного знания в области информационной безопасности, получение практических умений обеспечения защиты закрытых и открытых систем, создание условий для самоопределения учащихся к последующему обучению и профессиональной деятельности по специальностям информационной безопасности.

Задачи курса:

- познакомиться с ролью информационной безопасности в современном обществе, основой правовых и этических аспектов использования компьютерных программ и работы в Интернете;
- получить навыки применения, анализа и преобразования информационных моделей реальных объектов и процессов; обеспечения защиты закрытых и открытых систем; эксплуатации уязвимостей открытых и закрытых систем для обеспечения безопасности корпораций и бизнеса с помощью киберполигона Ampire и решения CTF задач;
- развитие у обучающихся познавательных интересов, интеллектуальных и творческих способностей путем нестандартных и разнообразных решений задач по обеспечению безопасности систем;

- приобретение обучающимися знаний этических аспектов информационной деятельности и информационных коммуникаций в глобальных сетях;
- приобретение обучающимися знаний законов Российской Федерации, связанных с информационной деятельностью, информационными коммуникациями в глобальных сетях, государственной тайной и распространением персональных данных;
- осознание ответственности людей, вовлеченных в создание и использование информационных систем, распространение и использование информации.

Образовательные результаты

Освоение содержания учебной дисциплины «Введение в Кибербезопасность» обеспечивает достижение студентами следующих результатов:

личностных:

в сфере гражданского воспитания:

- сформированность гражданской позиции обучающегося как активного и ответственного члена российского общества;
- принятие традиционных национальных, общечеловеческих гуманистических и демократических ценностей;
- представление о видах идентичности, актуальных для становления человечества и общества, для жизни в современном поликультурном мире;
- готовность противостоять идеологии экстремизма, национализма, ксенофобии, дискриминации по социальным, религиозным, расовым, национальным признакам;
- умение взаимодействовать с социальными институтами в соответствии с их функциями и назначением; готовность к гуманитарной и волонтерской деятельности;

в сфере патриотического воспитания:

- сформированность российской гражданской идентичности, патриотизма, уважения к своему народу, чувства ответственности перед Родиной, гордости за свою страну, свой край, свой язык и культуру, прошлое и настоящее многонационального народа России;
- ценностное отношение к государственным символам, историческому и природному наследию, памятникам, традициям народов России, достижениям России в науке, технологиях, труде;

в сфере духовно-нравственного развития:

- сформированность нравственного сознания, этического поведения, способность оценивать ситуации нравственного выбора и

принимать осознанные решения, ориентируясь на морально-нравственные ценности и нормы современного российского общества;

- понимание значения личного вклада в построение устойчивого будущего;
- ответственное отношение к своим родителям, представителям старших поколений, осознание значения создания семьи на основе принятия ценностей семейной жизни в соответствии с традициями народов России;
- освоение гуманистических традиций и ценностей, уважение к личности, правам и свободам человека, культурам разных народов;

в сфере эстетического воспитания:

- представление об исторически сложившемся культурном многообразии своей страны и мира;
- эстетическое отношение к миру, современной культуре, включая эстетику быта, научного и технического творчества, спорта, труда, общественных отношений;

в сфере физического воспитания:

- осознание ценности жизни и необходимости ее сохранения;
- представление об идеалах гармоничного физического и духовного развития человека в исторических обществах и в современную эпоху;

в сфере трудового воспитания:

- понимание значения трудовой деятельности как источника развития человека и общества;
- уважение к труду и результатам трудовой деятельности человека;
- формирование интереса к различным сферам профессиональной деятельности;
- мотивация и способность к образованию и самообразованию на протяжении всей жизни;

в сфере экологического воспитания:

- осмысление исторического опыта взаимодействия людей с природной средой, его позитивных и негативных проявлений;

в понимании ценности научного познания:

- сформированность мировоззрения, соответствующего современному уровню развития исторической науки и общественной практики, основанного на диалоге культур, способствующего осознанию своего места в поликультурном мире;
- осмысление значения истории как знания о развитии человека и общества, о социальном и нравственном опыте предшествующих поколений;
- совершенствование языковой и читательской культуры как средства взаимодействия между людьми и познания мира;
- овладение основными навыками познания и оценки событий прошлого с позиций историзма, готовность к осуществлению учебной проектно-исследовательской деятельности в сфере истории;

- приобщение к истокам культурно-исторического наследия человечества, интерес к его познанию за рамками учебного курса и школьного обучения.

Работа на программе способствует также развитию *эмоционального интеллекта* школьников, в том числе *самосознания* (включая способность осознавать роль эмоций в отношениях между людьми); *саморегулирования,* включающего самоконтроль, умение принимать ответственность за свое поведение, способность адаптироваться к эмоциональным изменениям и проявлять гибкость, быть открытым новому; *внутренней мотивации*, включающей стремление к достижению цели и успеху, оптимизм, инициативность, умение действовать, исходя из своих возможностей; *эмпатии* (способность понимать другого человека, оказавшегося в определенных обстоятельствах); *социальных навыков* (способность выстраивать конструктивные отношения с другими людьми, регулировать способ выражения своих суждений и эмоций с учетом позиций и мнений других участников общения).

метапредметных:

- ***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 материала, объекта;
- владеть навыками учебно--исследовательской и проектной деятельности;
- выявлять характерные признаки явлений;
- раскрывать причинно--следственные связи; сравнивать события, ситуации, определяя основания для сравнения, выявляя общие черты и различия;
- формулировать и обосновывать выводы; соотносить полученный результат с имеющимся знаниями;
- определять новизну и обоснованность полученного результата;

- представлять результаты своей деятельности в различных формах (сообщение, эссе, презентация, реферат, учебный проект и другие);
- объяснять сферу применения и значение проведенного учебного исследования в современном общественном контексте;

работа с информацией:

- осуществлять анализ учебной и внеучебной информации (учебники, источники, научно--популярная литература, интернет -ресурсы и другие);
- извлекать, сопоставлять, систематизировать и интерпретировать информацию;
- различать виды источников 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 современном мире;
- 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 значение совместной деятельности людей как эффективного средства достижения поставленных целей;
- планировать и осуществлять совместную работу, коллективные учебные проекты, 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 другие;

владение приемами самоконтроля:

- осуществлять самоконтроль, рефлексию 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.

СОДЕРЖАНИЕ УЧЕБНОГО ПРЕДМЕТА «Введение в Кибербезопасность»:

Введение(1ч)

Роль информационной безопасности в современном обществе. Почему именно она? Что из себя представляет работа в сфере информационной безопасности.

Раздел 1. Знакомство с задачами информационной безопасности (9ч)

Тема 1.1. Введение в практические задачи информационной безопасности. Знакомство с Linux . (3ч)

Практическое занятие: Решение задач CTF и киберполигона, для показа различных областей информационной безопасности.

Тема 1.2.) Нормативно-правовая база обеспечения информационной безопасности (1ч)

Практическое занятие: На примере решенных задач показать какие законы могли нарушить без какой-либо доверенности, договора, лицензии.

Раздел 2. *Средства кибербезопасности* (15 ч)

Тема 2.1. Инъекции и Web. (2ч)

Разновидности инъекций и их смысл.

Последствия инъекций.

Способы ограничений инъекций.

Запросы.

Изменения запросов.

Аналитика Кода.
Поверхностное изучение JS, html, SQL, php.
Полезные утилиты и как ими пользоваться.
Кем можно работать и в каких отделах.
Диапазон ЗП.

Практическое занятие: Решение сценария на киберполигоне за команду защиты, команду атаки, решения задач CTF связанных с инъекциями.

Тема 2.2. Сетевые протоколы аутентификации и Криптография. (2ч)

Сетевые протоколы и их назначения.
Базовые шифры.
Полезные утилиты и как ими пользоваться.
Кем можно работать и в каких отделах.
Диапазон ЗП.

Практическое занятие: Решения задач CTF связанных с криптографией и решение сценариев на киберполигоне связанных с эксплуатации уязвимых протоколов.

Тема 2.3. Компьютерная криминалистика. (3ч)

Что такое компьютерная криминалистика.
Что будет являться доказательством преступления.
Полезные утилиты и как ими пользоваться.
Кем можно работать и в каких отделах.
Диапазон ЗП.

Тема 2.4. Стеганография. (2ч)

Что такое Стеганография.
Способы передачи и хранения информации.
Полезные утилиты и как ими пользоваться.
Кем можно работать и в каких отделах.
Диапазон ЗП.

Тема 2.5. OSINT. (2ч)

Что такое OSINT.
Поиск информации в интернете.
Метаданные.
Полезные утилиты и как ими пользоваться.
Кем можно работать и в каких отделах.
Диапазон ЗП.

Тема 2.6. Обратная разработка. (2ч)

Что такое Обратная разработка.

Языки программирования.
Полезные утилиты и как ими пользоваться.
Кем можно работать и в каких отделах.

Тема 2.7. PWN. (2ч)

Что такое PWN.
Полезные утилиты и как ими пользоваться.
Эксплойты.
Кем можно работать и в каких отделах.
Диапазон ЗП.

Практическое занятие: Решение сценариев на киберполигоне связанных с расследованием и нахождением доказательств.

Раздел 3. Подготовка к киберучениям и CTF. (11ч.)

Тема 3.1.Создание команды.(1ч)

Ученики разделяться на команды по 4-6 человек.
Выбор командира.
Разделение обязанностей.

Тема 3.2. Командное решение сценариев киберполигона, командное решение CTF их его разбор. (10ч)

Практическое занятие: Решение сценария №1 на киберполигоне Ampire. Разбор заданий.

Практическое занятие: Решение T-CTF 2024 года. Разбор заданий.

Практическое занятие: Решение сценария №2 на киберполигоне Ampire. Разбор заданий.

Практическое занятие: Решение Pico-CTF 2024 года. Разбор заданий.

Практическое занятие: Решение сценария №3 на киберполигоне Ampire. Разбор заданий.

Практическое занятие: Решение КиберКолизея-CTF 2024 года. Разбор заданий.

Практическое занятие: Решение сценария №4 на киберполигоне Ampire. Разбор заданий.

Практическое занятие: Решение SIB-CTF 2024 года. Разбор заданий.

Практическое занятие: Решение сценария №5 на киберполигоне Ampire. Разбор заданий.

Практическое занятие: Решение PatriotCTF 2023 года. Разбор заданий.

Тематическое планирование

№ п/п	Тема	Количество часов
	Введение	**1**
1	**Раздел 1. Знакомство с разделами информационной безопасности**	**4**
	Тема 1.1. Поверхностное знакомство с задачами каждого раздела информационной безопасности и их разбор. Знакомство с Linux .	3
	Тема 1.2. Законы по информационной безопасности часть 1.	1
2	**Раздел 2. Погружение в задачи по кибербезопасности**	**15**
	Тема 2.1. Инъекции и Web.	2
	Тема 2.2. Сетевые протоколы аутентификации и Криптография.	2
	Тема 2.3. Компьютерная криминалистика.	3
	Тема 2.4. Стеганография.	2
	Тема 2.5. OSINT.	2
	Тема 2.6. Обратная разработка.	2
	Тема 2.7. PWN.	2
	Работа над ошибками. Индивидуальная работа со школьниками. Зачет за первое полугодие	**1**
3	**Раздел 3. Разбиение на команды, подготовка к киберучениям и CTF**	**11**
	Тема 3.1.Создание команды.	1
	Тема 3.2. Командное решение сценариев киберполигона, командное решение CTF их его разбор.	10

4	**Повторение**	**2**
	Итоговое повторение. Предложения по участию в олимпиадах летом.	1
	Итоговое занятие. Аттестация за второе полугодие	1
	Итого:	**34**

Формы работы

Основной формой проведения занятий являются практические занятия, индивидуальное и коллективное выполнение заданий и прохождение сценария на киберполигоне, которые в зависимости от конкретной цели занятия могут варьироваться по формам работы и видам деятельности. Разбираются особенности решения задач и сценариев на киберполигоне, проводится анализ решения, и рассматриваются различные методы и приемы решения.

В рамках спецкурса предлагается вариант разработки индивидуального проекта, на примере: Разработка уязвимого узла, создание собственной базы задач по CTF, Разработка и внедрение пентестерского ПО. Разработка средств защиты.

Оценивание

Текущий контроль

Текущий контроль усвоения материала осуществляется путем оценивания прохождения сценария на киберполигоне. Сценарий на киберполигоне оценивается по критериям: время прохождения, подробности карточки уязвимости, эффективность закрытой уязвимости. Периодически знания и умения по пройденным темам проверяются тематическими тестовыми заданиями.

Итоговая аттестация

Итоговая аттестация проводится в конце периода обучения, на последнем занятии. Основой для итоговой аттестации служат результаты промежуточной аттестации, успеваемости учащегося.

Учебно-методическая литература:

Основные источники:

1. Гостев А.В. «Информационная безопасность: Учебное пособие». М.: Академия, 2020.
2. Касперский Е.В. «Основы криптографии». М.: Бином, 2018.

3. Иванов И.И. «Методы и средства защиты информации». СПб.: Питер, 2019.
4. Петров П.П. «Тестирование на проникновение». М.: Альпина Паблишер, 2021.
5. Сидоров С.С. «Кибербезопасность: Практическое руководство». М.: ДМК Пресс, 2022.

Интернет-ресурсы

Kaspersky Cybersecurity Awareness: www.kaspersky.com - Образовательный портал по вопросам кибербезопасности.

Khan Academy: www.khanacademy.org - Образовательные материалы по компьютерной науке и кибербезопасности.

OWASP (Open Web Application Security Project): www.owasp.org - Ресурсы по безопасности веб-приложений.

NIST (National Institute of Standards and Technology): www.nist.gov - Ресурсы по стандартам и руководствам в области кибербезопасности.