Муниципальное автономное общеобразовательное учреждение
Белоярского района «Средняя общеобразовательная школа № 3 г. Белоярский»

Рассмотрена на заседании
педагогического совета школы
Протокол от 16.12.2024 года №6

Утверждена приказом
СОШ №3 г. Белоярский
Протокол от 16.12.2024 года №840

Дополнительная общеобразовательная общеразвивающая программа технической направленности «Информационная безопасность. Криптография»

Возраст обучающихся: 15-18 лет
Срок реализации: 1 год

Автор-составитель:
Терехов Антон Владимирович,
учитель информатики

Белоярский, 2024

Пояснительная записка

Дополнительная общеобразовательная общеразвивающая программа «Информационная безопасность. Криптография» (далее – программа) имеет техническую направленность и разработана для воспитания технически грамотной и творческой личности, а также формирования у обучающихся устойчивого интереса к деятельности, направленной на получение и применение новых знаний для решения технологических, инженерных, творческих, исследовательских и прикладных задач.

Понятие «Безопасность» охватывает широкий круг интересов, как отдельных лиц, так и целых государств. В наше мобильное время цифровых технологий, когда интернет проник во все сферы деятельности человека: начиная от пересылки SMS и заканчивая базами данных огромных предприятий и организаций, системами управления автоматизированными процессами запусками ракет и т.д., видное место отводится проблеме информационной безопасности, обеспечению защиты конфиденциальной информации.

Одним из способов защиты информации заключался в преобразовании смыслового текста в некий набор хаотических знаков (или букв алфавита). Получатель данного донесения имел возможность преобразовать его в то же самое осмысленное сообщение, если обладал ключом к его построению. Этот способ защиты информации называется криптографическим. Криптография – (от др.-греч. κρυπτός - скрытый и γράφω - пишу) - «скрыто пишу». По утверждению ряда специалистов криптография по возрасту - ровесник египетских пирамид. В документах древних цивилизаций - Индии, Египта, Месопотамии - есть сведения о системах и способах составления шифрованных писем.

Новизна программы заключается в формировании у будущих специалистов компетенций в области обеспечения информационной безопасности, правовых аспектов информационной безопасности, кибербезопасности, а также получения базовых знаний по криптографии и элементам сетевой безопасности, обеспечения информационной безопасности личного пространства. Программа адаптирована для старшего возраста обучающихся, собирающихся осуществлять исследовательскую, проектную и инженерную деятельность.

Актуальность данной программы состоит в том, что последнее время сообщения об атаках на информацию, о хакерах и компьютерных взломах наполнили все средства массовой информации. Дать определение этому действию на самом деле очень сложно, поскольку информация, особенно в электронном виде, представлена сотнями различных видов.

С массовым внедрением компьютеров во все сферы деятельности человека объем информации, хранимой в электронном виде, вырос в тысячи раз. А с появлением компьютерных сетей даже отсутствие физического доступа к компьютеру перестало быть гарантией сохранности информации.

Педагогическая целесообразность программы заключается в том, что в рамках реализации обучающиеся получать метазнания, то есть способность оперировать методами и приемами познания, и метаумения - навыки практического мышления, систематизации и обобщения, анализа информации, критического и технического мышления, а также поиска альтернативных вариантов достижения поставленных целей.

Наряду с этим использование различных инструментов развития гибких навыков обучающихся (игропрактика, командная работа) в сочетании с развитием у них предметных умений позволит сформировать у школьника целостную систему знаний, умений и навыков.

Данная программа состоит из 6 модулей:

- Введение в профессию «Белый хакер – пентестер».
- Разведка в сети.
- Атака первичного доступа.
- Закрепление доступа и повышение привилегий.
- Проброс сетевого трафика.
- Противодействие обнаружению. Развитие хакера

Отличительная особенность программы состоит в освоении трёх типов содержания: мировоззренческого, знаниевого и деятельностного. В области мировоззрения программа

предполагает переход от ценности потребления к развитию, далее – к развитию науки. В области знания предполагается расширение имеющегося знания до современного предметного знания, далее – работа в проблемных, открытых естественнонаучных областях и смежных науках.

В деятельности предлагается применять полученные информационные знания в практических сферах и проектах, что особенно важно при анализе при работе на стыке нескольких предметов.

Направленность программы – техническая.

Уровень освоения программы – базовый. Формирование и развитие творческих способностей детей, формирование общей культуры учащихся; удовлетворение индивидуальных потребностей в интеллектуальном, нравственном и физическом совершенствовании, формирование культуры здорового и безопасного образа жизни, укрепление здоровья, а также на организацию их свободного времени.

Целевая аудитория

Характеристики обучающихся, возрастные особенности, иные медико-психолого-педагогические характеристики

Программа рассчитана на обучение и развитие обучающихся 15-18лет. Подростка отличает стремление к самостоятельности, независимости, к самопознанию, формируются познавательные интересы. Задача педагога доверять подростку решение посильных для него вопросов, уважать его мнение. Общение предпочтительнее строить не в форме прямых распоряжений и назиданий, а в форме проблемных вопросов. У подростка появляется умение ставить перед собой и решать задачи, самостоятельно мыслить и трудиться. Подросток проявляет инициативу, желание реализовать и утвердить себя. В этот период происходит окончательное формирование интеллекта, совершенствуется способность к абстрактному мышлению. Для старшего подростка становится потребностью быть взрослым. Проявляется стремление к самоутверждению себя в роли взрослого.

Задача педагога побуждать обучающегося к открытию себя как личности и индивидуальности в контексте художественного творчества, к самопознанию, самоопределению и самореализации. Совместная деятельность для школьников этого возраста привлекательна как пространство для общения. Для возрастной категории 15-18 лет при решении кейсов и разработке проектов предусмотрены задания повышенного уровня сложности, применяется оборудование, соответствующее возрасту. В программе запланировано проведение комбинированных (смешанных) занятий: занятия состоят из теоретической и практической частей, причём большее количество времени занимает именно практическая часть. Это связано с тем, что основная цель программы состоит в том, чтобы дать обучающемуся как можно больше практических знаний и сформировать как можно больше практических умений.

Форма обучения: очная, очная с применением дистанционных технологий.

Особенности организации образовательного процесса

Учащиеся организуются в учебную группу постоянного состава. Формы занятий: групповые (10-15 человек). Отбор содержания основан на принципах научности, доступности, преемственности, практической направленности, учитывает возрастные особенности учащихся.

Практические занятия будут направлены на решение расчетных и практических задач. Создание мини-проекта предполагает знакомство с технологией ведения проектной деятельности. На занятиях ученик будет попробовать себя в специфических видах деятельности, присущих информатики (планирование, проведение эксперимента и обработка полученных результатов, решение более сложных расчетных, экспериментальных и качественных задач). При организации занятий предусматривается использование следующих методов и видов обучения:

1) словесный метод выражается в разъяснениях заданий, непонятных моментов, в рассказах о примерах проявлений изучаемых явлений в нашей жизни и практике, в больших лекциях по углублению уже полученных знаний, в дискуссиях по вопросам занятий;

2) наглядный метод в демонстрации программ процессов, и т.д.;
3) практический метод реализуется безопасном поведении при работе с компьютерными программами, информацией в сети интернет
4) частично-поисковый, исследовательский метод - через выполнение мини-проекта и выполнения практических задания.

Программа основана на следующих принципах: доступности, наглядности, системности, последовательности.

Для подготовки к выступлениям, соревнованиям могут быть объединены обучающиеся разных групп.

Содержание программы предусматривает развитие творческих способностей детей, формирование начальных информационных знаний, навыков, умений, способствует приобретению чувства уверенности и успешности, психологического благополучия, навыков разбиения задачи на подзадачи, работы в команде, ведения мозгового штурма, применения логического и аналитического мышлений, навыков по работе с современными программами в области информационных технологий и машинного обучения.

Сроки освоения программы и её объём

Программа рассчитана на 1 год обучения, объём программы 72 часа.

Цель программы – сформировать у обучающихся компетенций в областях: обеспечение информационной безопасности; правовые аспекты информационной безопасности; криптография; сетевая безопасность; безопасность личного информационного пространства; обеспечение условий для профилактики негативных тенденций в развитии информационной культуры учащихся, повышения защищённости детей от информационных рисков и угроз; формирование навыков своевременного распознавания онлайн-рисков (технического, контентного, коммуникационного, потребительского характера.

Задачи программы:

Обучающие:

- создать условия для формирования умений, необходимых для различных форм безопасной коммуникации (электронная почта, чаты, блоги, форумы, социальные сети и др.) с различными целями и ответственного отношения к взаимодействию в современной информационно-телекоммуникационной среде;
- дать представление о видах и способах распространения вредоносных кодов, способов защиты личных устройств;
- познакомить со способами защиты от противоправных посягательств в Интернете, защиты личных данных;
- познакомить со стандартами информационного взаимодействия систем;
- познакомить с конструкциями типичных элементов линий передачи информации;
- сформировать умения задавать базовые параметры, в том числе параметры защиты от несанкционированного доступа к операционным системам, а так же настройки конфигурации операционных систем сетевых устройств;
- познакомить с архитектурой, устройством и функционированием вычислительных систем;
- сформировать знания в области обеспечения защиты информации в вычислительных сетях и системах;
- сформировать знания в области типовых и программно-аппаратных средств защиты информации в операционных системах.

Развивающие:

- развивать мыслительные, творческие, коммуникативные способности;
- развивать творческую инициативу и самостоятельность.

Воспитательные:

- Воспитать культуру общения и поведения в сетевом пространстве;
- Воспитать целеустремлённость личности;
- Воспитать толерантную и культурную личность;

- Воспитывать дисциплинированность, ответственность, самоорганизацию;
- Воспитать трудолюбие, уважение к труду;
- Формировать чувство коллективизма и взаимопомощи;
- Способствовать раскрытию внутреннего мира обучающихся;
- Формировать новаторское отношение ко всем сферам жизнедеятельности человека;
- Воспитывать самостоятельность в приобретении дополнительных знаний и умений;
- Воспитывать дисциплинированность, ответственность, самоорганизацию;
- Воспитать трудолюбие, уважение к труду;
- Формировать чувство коллективизма и взаимопомощи;
- Способствовать раскрытию внутреннего мира обучающихся;
- Формировать новаторское отношение ко всем сферам жизнедеятельности человека;
- Воспитывать самостоятельность в приобретении дополнительных знаний и умений;
- Воспитывать чувство патриотизма, гражданственности, гордости за достижения отечественной науки и техники.

Принципы реализации программы:

- системность, целостность, объективность, научность, доступность для обучающихся, реалистичность, практическая направленность;
- комплексность и взаимосвязь всех факторов, влияющих на процесс воспитания;
- единство восприятия, обучения, развития;
- сочетание педагогического руководства с развитием активности, самостоятельности и инициативы учащихся;
- системность и последовательность образования и воспитания;
- учет возрастных индивидуальных особенностей обучающегося

Формы реализации программы

Программа реализуется в очной форме. В целях оказания содействия лицам, которые проявили выдающиеся способности, показавшим высокий уровень интеллектуального развития и творческих способностей возможна организация образовательного процесса по индивидуальному учебному плану. В ходе реализации программы применяются различные современные образовательные технологии, в том числе дистанционные образовательные технологии, электронное обучение; предпочтение отдается активным формам и методам обучения (экскурсии, подготовка и защита творческих проектов, интеллектуальные игры, круглые столы и т.д.), вместе с тем осуществляются и традиционные формы образовательной деятельности (эвристическая беседа, лекции, практические работы и т.д.).

Результаты обучения:

- Защита творческих проектов, обучающихся;
- Участие в конкурсах;
- Публикации обучающихся;
- Мониторинг учебных достижений, обучающихся;
- Отчеты по практическим, экспериментальным работам обучающихся;
- Защита исследовательских работ.

Прогнозируемый результат освоения программы

должны знать:

- основные правовые аспекты использования компьютерных программ и работы в Интернете;
- о влиянии информационных технологий на жизнь человека в обществе;
- об «операционных системах» и основных функциях операционных систем;
- об общих принципах разработки и функционирования интернет-приложений;
- о компьютерных сетях и их роли в современном мире;
- приемы безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.

должны уметь:

- безопасно использовать средства коммуникации;
- безопасно использовать ресурсы интернета;
- идентифицировать типичные инциденты;
- задавать базовые параметры, в том числе параметры защиты от несанкционированного доступа к операционным системам;
- настраивать и управлять сетевыми устройствами;
- использовать процедуры восстановления данных;
- определять точки восстановления данных;
- производить мониторинг администрируемых сетевых устройств информационно-коммуникационных систем;
- применять внешние программно-аппаратные средства для контроля производительности сетевой инфраструктуры;
- устанавливать и настраивать параметры сетевых протоколов, реализованных в телекоммуникационном оборудовании;
- применять программно-аппаратные средства защиты информации в операционных системах;
- применять антивирусные средства защиты информации в операционных системах;
- анализировать компьютерную систему с целью определения уровня защищенности;
- использовать типовые криптографические средства защиты информации;
- классифицировать и оценивать угрозы информационной безопасности;
- изготавливать защищенное техническое средство или систему обработки информации.

УЧЕБНЫЙ ПЛАН

№ п/п	Наименование модулей	Кол-во часов
1	Введение в профессию «Белый хакер – пентестер»	4
2	Разведка в сети.	12
3	Атака первичного доступа	24
4	Закрепление доступа и повышение привилегий.	12
5	Проброс сетевого трафика.	12
6	Противодействие обнаружению. Развитие хакера.	8
	Всего часов:	**72**

Модуль 1. Введение в профессию «Белый хакер – пентестер»

Вводное занятие.

Теория:

Одним из необходимых навыков в современном мире является поиск информации в Интернете.

Для пентестера этот навык является ключевым, так как такому специалисту необходимо не только постоянно совершенствовать свои знания и осваивать новые рабочие инструменты, но и следить за новыми тенденциями в мире кибербезопасности, а также своевременно разобраться в новых техниках и тактиках злоумышленников.

Практика:

1. Потребуется регистрация на платформе.
2. Даже если сдали флаг в облачной платфоме, потребуется сдать его ещё и в stepik'e.
3. Для доступа к некоторым стендам потребуется воспользоваться openVPN.

4. Выполнять задания через ОС Kali Linux удобнее, поэтому всё равно она потребуется и желательно развернуть ОС локально (обычно это делается через VirtualBox).

Модуль 2. Разведка в сети.

Теория:

Разведка в сети – это процесс сбора информации об объекте или цели в интернете. Это может быть любая информация, которая может помочь в осуществлении дальнейших действий по отношению к объекту. Например, определение уязвимостей или сбор данных для атаки.

Инфраструктура компании - это совокупность аппаратных, программных и сетевых средств, используемых для поддержания бизнес-процессов и обеспечения безопасности информации, находящейся в распоряжении компании. Она включает в себя серверы, сетевые устройства, базы данных, приложения и другие компоненты, используемые для обработки, хранения и передачи данных. Эффективная инфраструктура компании должна быть разработана с учетом требований к безопасности и включать в себя меры защиты, которые обеспечат целостность, конфиденциальность и доступность информации в пределах организации.

Сетевой сканер - это программа, предназначенная для сканирования компьютерных сетей и обнаружения устройств, портов и служб, работающих на этих устройствах. Они используются для проверки безопасности сетей, выявления уязвимостей и проверки соответствия настроек безопасности определенным стандартам.

Доменное имя – это уникальное текстовое имя, которое используется для идентификации адреса ресурса в Интернете.

Практика:

Основной домен организации `cyber-ed.ru`. Задача постараться найти как можно больше поддоменов, связанных с этой организацией.

Некоторые поддомены в TXT-записи DNS-сервера содержат различные флаги. В одном из поддоменов (кстати, его имя будет логически связано с заданием) будет TXT-запись с флагом в формате: `FLAG=значение_флага`, где «значение_флага» - это смесь из 32 произвольных букв и цифр. Необходимо найти этот флаг и предоставить его значение в текстовое поле ниже.

Модуль 3. Атака первичного доступа.

Теория:

Атака первичного доступа (англ. Initial Access Attack) - это попытка несанкционированного доступа к системе, сети или приложению, с целью получить начальный уровень доступа и проникнуть в них.

Уязвимости - это слабые места в системе или приложении, которые могут быть использованы злоумышленниками для проведения атак.

Фишинг (Phishing) - это метод социальной инженерии, при котором злоумышленник пытается получить доступ к чужой информации, обманывая пользователей с помощью поддельных веб-сайтов, электронных писем или сообщений.

Фишинговый сервис - это специальный инструмент, который используется для проведения фишинг-атак.

Отказ в обслуживании (англ. *denial-of-service attack (DoS)*) – атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых пользователи системы не смогут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ будет затруднён.

Атака «человек посередине» (англ. Man in the middle (MiTM)) - вид атаки в компьютерной безопасности, когда злоумышленник тайно ретранслирует и при необходимости изменяет связь между двумя сторонами, которые считают, что они непосредственно общаются друг с другом.

Практика:

Проанализируйте веб-приложение, развернутое по адресу `http://localhost:1337`. Обнаружить версию ПО и его наименование, определить наличие в данном ПО известных уязвимостей при помощи фреймворка Metasploit. Проэксплуатировать известную уязвимость, имеющуюся в используемом приложением фреймворке.

Модуль 4. Закрепление доступа и повышение привилегий.

Теория:

Закрепление доступа - это набор методов, которые атакующие используют для сохранения доступа к системам после перезагрузки, изменения учетных данных и других изменений, которые могли бы прервать их доступ.

Backdoor *(англ. Тайная дверь)* - Backdoor - это скрытый способ доступа к системе, приложению или устройству, который обычно используется для обхода стандартных механизмов аутентификации и безопасности.

MITRE ATT&CK *(Adversarial Tactics, Techniques, and Common Knowledge)* - матрица для описания тактик, техник и процедур, которые могут использоваться киберпреступниками для осуществления кибератак на организации и компании. MITRE ATT&CK описывает более 200 тактик и приемов, которые могут использоваться киберпреступниками на разных этапах кибератаки: от получения доступа к сети до уничтожения данных и скрытия следов своей деятельности.

Практика:

Проэксплуатировать уже известные вам уязвимости приложения, развернутого по адресу http://localhost:1337. Теперь, после эксплуатации уязвимостей сгенерировать нагрузку для закрепления доступа в системе при помощи утилиты pupy. Отправить эту нагрузку на скомпрометированную систему и запустить ее там.

В качестве подтверждения успешной эксплуатации предоставить информацию, которую выводит сгенерированная и запущенная в уязвимой системе нагрузка при помощи команды `info`.

Модуль 5. Проброс сетевого трафика.

Теория:

Pivoting (англ. Pivot – «точка опоры») – набор техник, с помощью которых организовывается доступ к тем сетям, к которым нет доступа при обычных обстоятельствах. При этом доступ получен с использованием скомпрометированных компьютеров.

Прокси-сервер (англ. «Proxy») - промежуточный сервер в компьютерных сетях, выполняющий роль посредника между пользователем и целевым сервером, позволяющий клиентам как выполнять косвенные запросы к другим сетевым службам, так и получать ответы.

Туннелирование в компьютерных сетях (англ. «Tunneling») - процесс, в ходе которого создается логическое соединение между двумя конечными точками посредством инкапсуляции различных протоколов.

Переадресация портов (англ. «Port Forwarding») - проброс портов, который также иногда называемый перенаправлением портов или туннелированием – это процесс пересылки трафика, адресованного конкретному сетевому порту с одного сетевого узла на другой. **Port2Port (также известный как P2P)** - это техника перенаправления сетевого трафика между двумя различными портами на одном и том же компьютере или между двумя разными компьютерами.

Port2Hostnet - это техника перенаправления сетевого трафика через порт в сеть удаленного узла.

Практика:

В этой задаче присутствует два узла и два веб-сервера. Назовем их *jump* и *target*.

Вам предоставлен доступ к веб-приложению на узле *jump*. Он откроется у вас по адресу `localhost:1337`.

Также доступен порт *1338*.

Проанализируйте защищенность панели расположенной на сайте узла jump и проэксплуатируйте найденные уязвимости, используя различные инструменты, описанные в шаге (помимо gost можно воспользоваться netcat и т.д.). Обнаружьте узел *target* в той же сети, где находится jump узел (узел target недоступен вам на прямую). Когда найдете узел *target*, проанализируйте веб-приложение target и найдите в нем файлы, опубликованные в веб-сервере. Для этого научитесь пробрасывать трафик для сканирования через узел *jump* на узел *target*.

В качестве подтверждения успешной эксплуатации предоставьте флаг (секретную строку в формате 32 букв и цифр) из кода специальной скрытой страницы на узле *target*.

Модуль 6. Противодействие обнаружению. Развитие хакера.

Теория:

Endpoint Detection & Response (EDR) - класс решений для обнаружения и изучения вредоносной активности на конечных точках, подключенных к сети рабочих станциях, серверах, устройствах Интернета вещей и так далее. В отличие от антивирусов, задача которых бороться с типовыми и массовыми угрозами, EDR-решения ориентированы на выявление целевых атак и сложных угроз. При этом EDR-решения не могут полностью заменить антивирусы (EPP), поскольку эти две технологии решают разные задачи.

Endpoint Protection Platform (EPP) - комплексные защитные решения для конечных точек, в которые входит антивирус, технологии шифрования данных, технологии для отслеживания и устранения уязвимостей, контроля приложений и устройств и т.д.

Security Information and Event Management (SIEM) - решения для сбора и автоматического анализа информации о событиях безопасности.

Next Generation Firewall, межсетевой экран нового поколения (NGFW) - межсетевой экран для глубокой фильтрации трафика, интегрированный с IDS (Intrusion Detection System, система обнаружения вторжений) или IPS (Intrusion Prevention System, система предотвращения вторжений), и обладающий возможностью контролировать и блокировать трафик на уровне приложений.

Intrusion Detection System (IDS) - система обнаружения вторжений, программный продукт или устройство, предназначенные для выявления несанкционированной и вредоносной активности в компьютерной сети или на отдельном хосте. Задача IDS - обнаружить проникновение киберпреступников в инфраструктуру и сформировать оповещение безопасности (функций реагирования, например блокировки нежелательной активности, в таких системах нет), которое будет передано в SIEM-систему для дальнейшей обработки.

Песочница - специально выделенная (изолированная) среда для безопасного исполнения компьютерных программ.

«Белые шляпы» (или «белые хакеры») - это специалисты по информационной безопасности, которые используют свои навыки и знания, чтобы обнаруживать уязвимости и слабые места в системах безопасности компьютеров и сетей, чтобы предотвращать кибератаки и другие виды злоупотреблений с целью защиты компаний, организаций и пользователей от потенциальных угроз.

«Черные шляпы» (или «нелегальные хакеры») - это хакеры, которые нарушают законы, взламывая системы безопасности компьютеров и сетей с целью получения несанкционированного доступа к чужим данным, финансовым ресурсам или другой ценной информации. Они используют свои навыки для получения выгоды, нанесения вреда или реализации других криминальных действий.

Практика:

Процесс ротации (смены) IP адресов необходим в работе пентестера, так как постоянная работа с активным анализом инфраструктуры приводит случаям блокирования вашего узла сети. Из-за этого приходится менять IP адрес, с которого вы выполняете активные действия.

Учебно-тематический план

№ урока	Тема	Кол-во часов
	Введение в профессию «Белый хакер – пентестер»	**4**
1	Введение в курс	1
2	Белый хакинг	3
	Разведка в сети.	**12**
3	Поиск доменных имен организации	2
4	Сканеры сети	2
5	Сканеры портов	2
6	Сканирование узлов сети	2
7	Практика «Разведка во внешней сети»	3
8	Тест по теме «Сканирование узлов сети»	1
	Атака первичного доступа	**24**
9	Уязвимости обхода аутентификации	3
10	Тест «Уязвимости обхода аутентификации»	1
11	Уязвимости контроля доступа	2
12	Практика. Уязвимости контроля доступа	3
13	Тест «Уязвимости контроля доступа»	1
14	Атаки межсайтового скриптинга (XSS)	2
15	Практика. Атаки межсайтового скриптинга (XSS)	3
16	Тест «Атаки межсайтового скриптинга»	1
17	Эксплуатация уязвимостей 1-го дня в сетевых сервисах.	2
18	Поиск email-адресов сотрудников организации	2
19	Практика. Поиск email-адресов сотрудников организации	3
20	Тест «Поиск email-адресов сотрудников организации»	1
	Закрепление доступа и повышение привилегий	**12**
21	Получение легитимного доступа к системе.	2
22	Практика. Получение легитимного доступа к системе.	3
23	Тест по теме «Получение легитимного доступа к системе.»	1
24	Эксплуатация ошибок администрирования ОС Linux	2
25	Практика. Эксплуатация ошибок администрирования ОС Linux	3
26	Тест «Эксплуатация ошибок администрирования ОС Linux»	1
	Проброс сетевого трафика	**12**
27	Использование стандартных протоколов для проброса трафика	2
28	Практика. Использование стандартных протоколов для проброса трафика	2
29	Обнаружение Windows-машин в сети	2
30	Компрометация Windows-машин в сети	2
31	Практика. Компрометация Windows-машин в сети	3
32	Тест «Компрометация Windows-машин в сети»	1
	Противодействие обнаружению. Развитие хакера	**8**
33	Направления развития	2

34	Этика	2
35	Практика. Криптография	3
36	Итоговый тест	1

Календарный учебный график

№ урока	Дата	Время проведения	Тема занятия	Кол-во часов	Форма занятия
1.			Введение в курс	1	Лекции
2.			Введение в курс	1	Дискуссии
3.			Белый хакинг	1	Лекции
4.			Белый хакинг	1	Дискуссии
5.			Поиск доменных имен организации	1	Лекции
6.			Поиск доменных имен организации	1	Лекции
7.			Сканеры сети	1	Лекции
8.			Сканеры сети	1	Дискуссии
9.			Сканеры портов	1	Лекции
10.			Сканеры портов	1	Лекции
11.			Сканирование узлов сети	1	Лекции
12.			Сканирование узлов сети	1	Лекции
13.			Практика «Разведка во внешней сети»	1	Практическая работа
14.			Практика «Разведка во внешней сети»	1	Практическая работа
15.			Практика «Разведка во внешней сети»	1	Практическая работа
16.			Тест по теме «Сканирование узлов сети»	1	Тестирование
17.			Уязвимости обхода аутентификации	1	Лекции
18.			Уязвимости обхода аутентификации	1	Лекции
19.			Уязвимости обхода аутентификации	1	Дискуссии
20.			Тест «Уязвимости обхода аутентификации»	1	Тестирование
21.			Уязвимости контроля доступа	1	Лекции
22.			Уязвимости контроля доступа	1	
23.			Практика. Уязвимости контроля доступа	1	Практическая работа
24.			Практика. Уязвимости контроля доступа	1	Практическая работа
25.			Практика. Уязвимости контроля доступа	1	Практическая работа
26.			Тест «Уязвимости контроля доступа»	1	Тестирование
27.			Атаки межсайтового скриптинга (XSS)	1	Лекции
28.			Атаки межсайтового скриптинга (XSS)	1	Дискуссии
29.			Практика. Атаки межсайтового скриптинга (XSS)	1	Практическая работа
30.			Практика. Атаки межсайтового скриптинга (XSS)	1	Практическая работа
31.			Практика. Атаки межсайтового скриптинга (XSS)	1	Практическая работа

32.			Тест «Атаки межсайтового скриптинга»	1	Тестирование
33.			Эксплуатация уязвимостей 1-го дня в сетевых сервисах	1	Лекции
34.			Эксплуатация уязвимостей 1-го дня в сетевых сервисах	1	Лекции
35.			Поиск email-адресов сотрудников организации	1	Лекции
36.			Поиск email-адресов сотрудников организации	1	Дискуссии
37.			Практика. Поиск email-адресов сотрудников организации	1	Практическая работа
38.			Практика. Поиск email-адресов сотрудников организации	1	Практическая работа
39.			Практика. Поиск email-адресов сотрудников организации	1	Практическая работа
40.			Тест «Поиск email-адресов сотрудников организации»	1	Тестирование
41.			Получение легитимного доступа к системе	1	Лекции
42.			Получение легитимного доступа к системе	1	Лекции
43.			Практика. Получение легитимного доступа к системе	1	Практическая работа
44.			Практика. Получение легитимного доступа к системе	1	Практическая работа
45.			Практика. Получение легитимного доступа к системе	1	Практическая работа
46.			Тест по теме «Получение легитимного доступа к системе»	1	Тестирование
47.			Эксплуатация ошибок администрирования ОС Linux	1	Лекции
48.			Эксплуатация ошибок администрирования ОС Linux	1	Лекции
49.			Практика. Эксплуатация ошибок администрирования ОС Linux	1	Практическая работа
50.			Практика. Эксплуатация ошибок администрирования ОС Linux	1	Практическая работа
51.			Практика. Эксплуатация ошибок администрирования ОС Linux	1	Практическая работа
52.			Тест «Эксплуатация ошибок администрирования ОС Linux»	1	Тестирование
53.			Использование стандартных протоколов для проброса трафика	1	Лекции
54.			Использование стандартных протоколов для проброса трафика	1	Лекции
55.			Практика. Использование стандартных протоколов для проброса трафика	1	Практическая работа
56.			Практика. Использование стандартных протоколов для проброса трафика	1	Практическая работа
57.			Обнаружение Windows-машин в сети	1	Лекции
58.			Обнаружение Windows-машин в сети	1	Лекции

59.			Компрометация Windows-машин в сети	1	Лекции
60.			Компрометация Windows-машин в сети	1	Дискуссии
61.			Практика. Компрометация Windows-машин в сети	1	Практическая работа
62.			Практика. Компрометация Windows-машин в сети	1	Практическая работа
63.			Практика. Компрометация Windows-машин в сети	1	Практическая работа
64.			Тест «Компрометация Windows-машин в сети»	1	Тестирование
65.			Направления развития	1	Лекции
66.			Направления развития	1	Лекции
67.			Этика	1	Лекции
68.			Этика	1	Лекции
69.			Практика. Криптография	1	Практическая работа
70.			Практика. Криптография	1	Практическая работа
71.			Практика. Криптография	1	Практическая работа
72.			Итоговый тест	1	Тестирование

Методические материалы

Данная программа одновременно формирует у учащихся языковую и научно-исследовательскую компетентность, предполагает изучение теоретического материала и выполнение практических заданий, способствующих усвоению и закреплению умений и навыков использования различной информации для формирования собственного мнения и прогнозирования деятельности. При выполнении практических заданий, помогающих раскрыть основные теоретические положения, необходимо подвести итог, сделать самостоятельный вывод о значении информационной безопасности во время занятий. Система занятий по данной программе включает дискуссии, в ходе которых перед обучающимися ставятся исследовательские задачи, что способствует формированию соответствующих умений, развитию высокого уровня активности, воспитанию личностного отношения к содержанию обучения в дистанционном обучении. Процесс обучения построен на принципе «от простого к сложному», с учетом возрастных особенностей обучающихся, доступности материала, развивающего обучения.

Виды контроля:

- вводный, который проводится перед началом работы и предназначен для закрепления знаний, умений и навыков по пройденным темам;
- текущий, проводимый в ходе занятия и закрепляющий знания поданной теме;
- итоговый, проводимый после завершения всей программы.

Формы проверки результатов:

- наблюдение за обучающимися в процессе работы;
- соревнования;
- индивидуальные и коллективные исследовательские проекты.

Формы подведения итогов:

- выполнение практических заданий (тесты) и лабораторных работ;
- творческое задание (подготовка проекта и его презентация).

Качество реализации программы отслеживается при помощи мониторинга результативности образовательной деятельности обучаемого, ориентированного на задачи программы.

Цель мониторинга: проверить и проанализировать сформированность следующих показателей:

1. Уровень усвоения теоретического материала и его практическое применение.
2. Стремление к самообразованию.
3. Способность формулировать и излагать свое мнение.
4. Ответственное отношение к выполнению проекта.

Критерии оценивания:

Уровень ниже заданного – практически не прослеживается освоение теоретического материала и качество выполнения практических заданий, не стремиться к самообразованию, не умеет формулировать и излагать свое мнение; не принимает участие в групповом проекте.

Низкий уровень – слабо прослеживается освоение теоретического материала и качество выполнения практических заданий, стремление к самообразованию, не уверенно формулирует и излагает свое мнение; практически не

принимает участие в групповом проекте.

Средний уровень – удовлетворительно (достаточно хорошо) прослеживается освоение теоретического материала и качество выполнения практических заданий, стремление к самообразованию, хорошо формулирует и излагает свое мнение; принимает участие в групповом проекте.

Высокий уровень – хорошо прослеживается освоение теоретического материала и качество выполнения практических заданий, стремление к самообразованию, отлично формулирует и излагает свое мнение; активно принимает участие в групповом проекте.

Уровень ниже заданного – 0, низкий уровень – 1, средний уровень – 2, высокий уровень – 3.

Для отслеживания и фиксации образовательных результатов используются:

- портфолио;
- фотоматериалы;
- материалы анкетирования и тестирования.

Портфолио является наиболее наглядной формой отслеживания и фиксации результатов. Портфолио включает общие сведения об учащемся, реферативное описание результативности работы в кружке, грамоты, дипломы, сертификаты о победах и участии в различных мероприятиях (конкурсах, выставках, соревнованиях), продукты деятельности (распечатку презентаций проектов и сами проекты), информацию, подтверждающую участие обучающегося в конкурсах и конференциях.

Защита портфолио является формой итоговой аттестации. Другими формами предъявления результатов деятельности обучающихся объединения служат:

Методы обучения по программе:

В методике приводится следующая классификация методов обучения: Пассивные: когда учитель доминирует, а учащиеся - пассивны. Такие методы используются на отдельных занятиях обучающего типа. Самый распространенный прием пассивных методов - лекция. Активные. Здесь учитель и ученик выступают как равноправные участники урока, взаимодействие происходит по вектору учитель = ученик. Интерактивные - наиболее эффективные методы, при которых ученики взаимодействуют не только с учителем, но и друг с другом. Вектор: учитель = ученик= ученик. Метод проектов предполагает самостоятельный анализ заданной ситуации и умение находить решение проблемы. Проблемный метод предполагает постановку проблемы (проблемной ситуации, проблемного вопроса) и поиск решений этой проблемы через анализ подобных ситуаций (вопросов, явлений). Эвристический метод объединяет разнообразные игровые приемы в форме конкурсов, деловых и ролевых игр, соревнований, исследований. Исследовательский метод перекликается с проблемным методом обучения. Только здесь учитель сам формулирует проблему. Задача учеников - организовать исследовательскую работу по изучению проблемы.

Педагогические технологии:

При реализации программы используются следующие педагогические технологии:

- технология группового обучения - для организации совместных действий, коммуникаций, общения, взаимопонимания и взаимопомощи;
- технология дифференцированного обучения – применяются задания различной сложности в зависимости от интеллектуальной подготовки учащихся;
- технология эдьютеймент – для воссоздания и усвоения обучающимися изучаемого материала, общественного опыта и образовательной деятельности;
- технология проблемного обучения – для творческого усвоения знаний, поэтапного формирования умственных действий, активизации различных операциймышления;
- технология проектной деятельности - для развития исследовательских умений; достижения определенной цели; решения познавательных и практических задач; приобретения коммуникативных умений при работе в группах;
- информационно-коммуникационные технологии – применяются для расширения знаний, выполнения заданий, создания и демонстрации презентаций назанятиях, проведения диагностики и самодиагностики.

Список использованной литературы

1. Закон РФ «Об образовании в РФ».

Методические материалы

2. https://ctfnews.ru/literature/
3. https://stepik.org/course/762/info
4. https://linux.die.net/man/1/gdb
5. https://www.asozykin.ru/courses/networks_online