Средняя общеобразовательная школа имени Героя Советского Союза Д.Н. Голосова с. Русская Борковка муниципального района Ставропольский Самарской области

СОГЛАСОВАНО

на педагогическом совете

Протокол № 1 от «30» 08. 2024 г.

УТВЕРЖДЕНО

к использованию в ГБОУ СОШ

с. Русская Борковка

Приказ № 246

от 30.08.2024

Директор_____

А.В.Миронова

Дополнительная общеобразовательная
общеразвивающая программа

«Кибербезопасность»

ЭП

C=RU, O=ГБОУ СОШ с.Русская Борковка, CN=Миронова А.В., E=r_borkov_sch@mail.ru
00cf2bb3e0198089d4
2024-08-30 11:49:36

Направленность: техническая
Возраст детей: 15- 18 лет

с. Русская Борковка

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Всеобщая цифровизация помимо безусловных преимуществ привнесла в современную жизнь высокие риски утечки данных, не предназначенных для постороннего использования. С развитием интернет-технологий, увеличением количества высокотехнологичных устройств, которыми мы себя окружаем, риск стать жертвой киберкриминала все больше увеличивается. Вместе с тем растет и важность кибербезопасности и как области информационных технологий, и как комплекса инструментов для обеспечения защиты конфиденциальных данных.

Кибербезопасность – состояние или процесс защиты компьютерных систем, направленный на отражение любых типов киберугроз, будь то действия вредоносных программ, разнообразные сетевые атаки вроде брутфорсинга и DDoS-атак или даже обучение персонала методам защиты от приемов социальной инженерии, фишинга и прочих уловок киберпреступников.

На сегодняшний день кибербезопасность превратилась в локомотив цифровизации, поскольку ни транспорт, ни энергетику, ни финансовый сектор, ни социальную сферу невозможно трансформировать в «цифру» без обеспечения информационной безопасности. И если раньше речь шла лишь о целостности, конфиденциальности и доступности данных, то сейчас это угроза захвата злоумышленниками управления различными устройствами, системами и даже целыми отраслями, поскольку благодаря всеобщей интернетизации все системы, включая цифровые фабрики, «умные» дома и «умные» города, объединены в единое киберпространство. И весь этот цифровой мир необходимо защищать от информационных и киберугроз, что делает кибербезопасность проблемой XXI века. Цифровое будущее не наступит без кибербезопасности.

Дополнительная общеобразовательная общеразвивающая программа «Кибербезопасность» (далее – Программа) технической направленности, базового уровня направлена на развитие интеллектуально-творческих способностей обучающихся, приобретение ими знаний и умений в области кибербезопасности и служит профориентационным средством.

Программа может быть использована при реализации проекта предпрофессионального образования «Школа старшеклассников», рекомендована обучающимся академических и IT-классов, а также при подготовке к участию в Чемпионате WorldSkills Russia, блок компетенций «Информационные и коммуникационные технологии».

Актуальность Программы заключается в создании условий для оптимального развития технических способностей обучающихся старших классов, их профессионального самоопределения. Она знакомит обучающихся с набором компетенций, необходимых специалисту по кибербезопасности: внимательность и аккуратность по работе с кодами, знание физических свойств в технических устройствах, аналитические навыки, умение просчитывать последствия изменений в системе, способность оперативно оценивать угрозы и их источник.

Специалист по кибербезопасности обеспечивает информационную защиту и выявляет угрозы потери данных. Профессионалы этой сферы работают в крупных IT-компаниях, финансовых организациях, правительственных органах, медицинских учреждениях и оборонных предприятиях. Их главная цель заключается не в отражении хакерской атаки, а в обеспечении перекрытия всех каналов доступа, чтобы этой самой атаки не произошло.

Новизна Программы заключается в практико-ориентированном подходе, основанном на применении игровых технологий обучения с использованием «виртуальных полигонов», моделирующих настоящие информационные и киберфизические системы и реальные кибератаки.

Данная Программа разработана на основе программы «Кибербезопасность» (разработчик Николаева Е.В., педагог дополнительного образования ГБПОУ «Воробьевы горы» г. Москва, 2020).

Педагогическая целесообразность Программы заключается в том, что она даёт сильный толчок для развития интеллекта обучающихся, формирует их логическое мышление, вырабатывает привычку аккуратной и систематической работы, помогает успешно овладевать не только общеучебными умениями и навыками, но и освоить более сложный уровень знаний.

Отличительная особенность Программы состоит в мотивации обучающихся к получению (в том числе самостоятельно) современных знаний как о средствах защиты, так и о механизмах реализации различных угроз. Программа разработана в соответствии с инновационным курсом сетевой академии Cisco «Cybersecurity Essetials», который не привязан к конкретному производителю оборудования, не является частью рекламы или маркетинга

какой-либо компании и носит социальный характер. Знания и навыки, полученные в результате освоения программы, особенно важны для современных подростков в связи с их активным использованием интернет-ресурсов и социальных платформ, для того чтобы иметь представление о типах киберугроз и уметь защитить и обезопасить себя и свои данные.

Цель Программы – познакомить обучающихся с основами кибербезопасности, стимулировать их интерес к профессиям, связанным с областью компьютерных технологий.

Реализация поставленной цели предусматривает решение ряда задач.

Задачи Программы

Обучающие:

- дать представление о типах вредоносного программного обеспечения, о методах его проникновения в систему;
- познакомить с отличительными чертами преступлений в сфере кибербезопасности;
- дать представление о тактике, методах и процедурах, используемых киберпреступниками;
- познакомить с основными принципами конфиденциальности, целостности и доступности относительно состояния данных и средств противодействия угрозам безопасности;
- обучать основным способам защиты конфиденциальности, обеспечения целостности и высокой доступности с помощью технологий, продуктов и процедур;
- дать представление о правовых аспектах деятельности специалиста по кибербезопасности;
- формировать умения использовать основные технологии, процессы и процедуры для защиты всех компонентов сетевой инфраструктуры.

Развивающие:

- развивать эффективное использование компьютерных систем;
- развивать мыслительные, творческие, коммуникативные способности обучающихся;
- развивать интеллектуальные и практические умения, самостоятельно приобретать и применять на практике полученные знания;
- развивать интерес к кибербезопасности как области профессиональной деятельности;
- развивать умения работать с разными источниками информации,

исследовательские и практические умения, коммуникативную культуру.

Воспитательные:

- содействовать социальной адаптации обучающихся в современном обществе, проявлению лидерских качеств;
- воспитывать устойчивый интерес к кибербезопасности;
- воспитывать информационную культуру обращения с данными;
- формировать потребность в творческой деятельности, стремление к самовыражению.

Категория обучающихся

Обучение по Программе ведется в разновозрастных группах, которые комплектуются из обучающихся 15–18 лет. Количество обучающихся в группе – 20 человек.

Сроки реализации Программы

Программа рассчитана на 1 год обучения. Общее количество часов в год составляет 34 часа.

Формы и режим занятий

Программа реализуется 1 раз в неделю по 1 часу. Программа включает в себя теоретические и практические занятия.

Планируемые результаты освоения Программы

По итогам реализации Программы обучающиеся будут

знать:

- основные типы интернет-угроз и уязвимостей;
- понятийный аппарат информационных технологий и особенности терминологии кибербезопасности;
- уровни обеспечения кибербезопасности;
- базовые составляющие в области развития систем информационной безопасности;
- основные способы защиты личности и персональных данных;
- объекты компьютерных технологий, используемые в обеспечении кибербезопасности;
- основные принципы криптографического шифрования данных;
- виды средств контроля целостности данных;
- алгоритмы устранения последствий нарушения целостности данных;
- роль и способы криптографической защиты.

По итогам реализации Программы обучающиеся будут

уметь:

- ориентироваться в огромном информационном поле;
- выявлять представляющие угрозу элементы;
- ставить цели, формулировать задачи, связанные с обеспечением кибербезопасности;
- анализировать тенденции развития систем обеспечения кибербезопасности;
- применять знания о кибербезопасности в решении поставленных задач;
- использовать знания о современных технологиях, применяемых в области кибербезопасности;
- использовать методы проведения анализа в области обеспечения кибербезопасности.

СОДЕРЖАНИЕ ПРОГРАММЫ

Учебный (тематический) план

	Название раздела/темы	**Количество часов**			**Формы аттестации и контроля**
		Всего	**Теория**	**Практика**	
1.	**Безопасность в цифровом Мире** Вводное занятие. Кибербезопасность. Ключевые концепции кибербезопасности. Техника безопасности	2	1	1	Первичная диагностика. Тестирование
2.	**Правовые аспекты защиты Киберпространства** Правовые акты в области информационных технологийи защиты киберпространства Государственная политика в области кибербезопасности	4	2	2	Текущий контроль. Практическая работа
3.	**Кибепреступность и Кибербезопасность** Киберпреступления Борьба с киберпреступностью	6	3	3	Текущий контроль. Практическая работа

4.	**Угрозы кибербезопасности, уязвимости и атаки** Угрозы Технические, социальные и физические атаки	6	3	3	Промежуточная аттестация. Тестирование
5.	**Способы защиты секретной Информации** Криптография	4	2	2	Текущий контроль. Практическая работа
7.	**Обеспечение целостности Данных** Хеш-функции Механизм HMAC Цифровая подпись	4	2	2	Текущий контроль. Практическая работа
8.	**Доступность систем и Сервисов** Повышение доступности систем и сервисов	2	1	1	Текущий контроль. Практическая работа
9	**Защита уровней обеспечения Кибербезопасности** Защита систем и устройств	4	2	2	
10	**Итоговая аттестация. Зачет**	2	-	2	Итоговая аттестация. Зачет
	Итого	34	16	18	

Содержание учебного (тематического) плана

Раздел 1. Безопасность в цифровом мире

Тема 1.1. Вводное занятие. Кибербезопасность. Ключевые концепции кибербезопасности. Техника безопасности

Теория. Знакомство с деятельностью объединения, с его целями и задачами, порядком и планом работы на учебный год. Инструктаж по технике безопасности.

Практика. Первичная диагностика. Тестирование.

Раздел 2. Правовые аспекты защиты киберпространства

Тема 2.1. Правовые акты в области информационных технологий и защиты киберпространства

Теория. Ответственность за киберпреступления. Конституционное право на поиск, получение и распространение информации. Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию». Информационное законодательство РФ. Закон РФ «Об информации, информационных технологиях и о защите информации». Уголовная ответственность за создание, использование и распространение вредоносных компьютерных программ. Правовые основы для защиты от спама. Правовые основы защиты интеллектуальной собственности. Авторское право. Правовая охрана программ для ЭВМ и БД. Лицензионное ПО. Виды лицензий (OEM, FPP, корпоративные лицензии, подписка). ПО с открытым кодом (GNU GPL, FreeBSD). Право на информацию, на сокрытие данных, категории информации. Персональные и общедоступные данные, ограниченный доступ. Закон «О персональных данных». Указ Президента РФ о создании действенной системы противодействия компьютерным атакам от

15 января 2013 г. Уголовный кодекс РФ, раздел «Преступления в сфере компьютерной информации».

Практика. Выполнение практических заданий по теме «Правовые акты в области информационных технологий и защиты киберпространства».

Тема 2.2. Государственная политика в области кибербезопасности

Теория. Доктрина информационной безопасности. Кибервойска. Защита киберпространства как одна из задач вооруженных сил. Информационная война. Информационное оружие. Информационное воздействие. Государственная, коммерческая тайна. Защита сайтов государственных органов (электронное правительство). Органы власти, отвечающие за защиту киберпространства.

Практика. Выполнение теста по темам раздела «Правовые аспекты защиты киберпространства».

Раздел 3. Кибепреступность и кибербезопасность

Тема 3.1. Киберпреступления

Теория. Понятие киберпреступления. Предпосылки киберпреступления. Особенности и виды киберпреступлений. Финансовые преступления. Фишинг. Фарминг. Кибер-порнография. Кибер-торговля наркотиками. Кибертерроризм. Азартные игры-онлайн. Киберпреследование. Социальная инженерия. Приемы манипуляции сознанием человека, их особенности. Социальное программирование. Социальное хакерство. Типовые угрозы и их распространение. Внутренние и внешние угрозы безопасности. Уязвимость мобильных устройств, интернет вещей.

Практика. Выполнение практических заданий. Определение типов киберугроз и методы противодействия киберпреступникам.

Тема 3.2. Борьба с киберпреступностью

Теория. Форензика – наука о раскрытии преступлений, связанных с компьютерной информацией. Исследование цифровых доказательств, методы поиска, получения и закрепления таких доказательств. Подготовка специалистов. Отдел по борьбе с киберпреступностью России. Конвенция о киберпреступности Совета Европы. Уголовный Кодекс РФ (УК РФ) глава «Преступления в сфере компьютерной информации» (статьи 272–274).

Практика. Выполнение практических заданий по теме «Борьба с киберпреступностью».

Раздел 4. Угрозы кибербезопасности, уязвимости и атаки

Тема 4.1. Угрозы

Теория. Базовые понятия информационной безопасности: угроза, уязвимость, атака, ущерб. Логическая связь между понятиями. Определение угрозы. Классификация угроз. Вредоносное программное обеспечение (ПО) и код. Вирусы. Сетевые черви. Социнженерийные трояны. Логические бомбы. Программы-вымогатели. Бэкдоры. Руткиты. Спуфинг. Тайпсквоттинг/кибersквоттинг. Криптоджекинг. Защита от вредоносных программ. Шпионское, рекламное программное обеспечение и поддельные антивирусные программы, спам. Методы обмана. Тактики социальной инженерии.

Практика. Промежуточная аттестация. Выполнение теста по теме «Угрозы».

Тема 4.2. Технические, социальные и физические атаки

Теория. Атака – одна из самых опасных угроз кибербезопасности. Четыре этапа атаки: рекогносцировка (recon), ловушка (hook), эксплуатация уязвимости (exploit), выход (exit). Фишинг и его формы. Претекстинг. Атаки «приманка». Метод «quid pro quo» (услуга за услугу). Физическая атака «Tailgating». Пять методов профилактики кибератак. Уменьшение поля атаки. Тщательная проверка критически важного персонала. Создание команды по обеспечению безопасности сети. Организация и использование ролевого доступа. Выбор надежных паролей.

Практика. Выполнение практических заданий. Обнаружение угроз и уязвимостей.

Раздел 5. Способы защиты секретной информации

Тема 5.1. Криптография

Теория. Задачи криптографии: обеспечить секретность, защитить целостность информации. Виды криптографической защиты информации: шифрование, стенография, кодирование, сжатие. Шифрование. Инструмент – алгоритм преобразования и ключ. Требования к методу шифрования. Типы криптографических преобразований. Симметричные алгоритмы шифрования. Асимметричные алгоритмы шифрования. Сравнение разных типов шифрования. Управление логическим доступом. Управление физическим доступом. Стратегии разграничения доступа. Идентификация: аутентификация, авторизация, отчетность. Средства контроля доступа. Методы сокрытия данных.

Практика. Выполнение практических заданий. Сравнение симметричного и асимметричного шифрования на практике, применение стенографии.

Раздел 6. Обеспечение целостности данных

Тема 6.1. Хеш-функции

Теория. Хеширование и свойства хэш-функций. Современные алгоритмы хеширования. Хеширование файлов и цифровых носителей. Хеширование паролей. Реализация механизма добавления «соли». Взлом хешей. Механизм HMAC: цели, принцип действия, реализация.

Практика. Выполнение практических заданий. Хеширование файлов и цифровых носителей.

Тема 6.2. Механизм HMAC

Теорбя. Механизм HMAC: цели, принцип действия, реализация. Псевдокод. Примеры кода.

Практика. Выполнбние практических заданий. Создание кода.

Тема 6.3. Цифровая подпись

Теория. Цифровые подписи и сертификаты. Технология цифровой подписи. Симметричная схема. Асимметричная схема. Виды ассиметричных алгоритмов. Модели атак и их возможные результаты. Проверка подлинности. Обеспечение целостности баз данных.

Практика. Выполнение практических заданий. Взлом пароля.

Раздел 7. Доступность систем и сервисов

Тема 7.1. Повышение доступности систем и сервисов

Теория. Доступность (основные понятия). Показатели эффективности. Угрозы доступности. Меры по повышению доступности. Asset Management. Многоуровневая защита. Резервирование. Отказоустойчивость системы. Реагирование на инциденты. Аварийное восстановление систем. Непрерывность бизнес-процессов.

Практика. Выполнение практических заданий. Резервирование маршрутизаторов и коммутаторов.

Раздел 8. Защита уровней обеспечения кибербезопасности

Тема 8.1. Защита систем и устройств

Теория. Повышение надежности хостов. Повышение надежности беспроводных и мобильных устройств. Защита данных на хостах. Управление содержимым и образами. Физическая защита рабочих станций. Повышение надежности сервера. Надежность сетевой инфраструктуры и методы ее защиты. Оборудование для передачи голоса и видео.

Практика. Выполнение практических заданий. Повышение надежности системы Ubuntu.

Раздел 9. Итоговое аттестация. Зачет

Практика. Итоговая аттестация. Зачет.

ФОРМЫ КОНТРОЛЯ И ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Формы контроля и оценочные материалы служат для определения результативности освоения обучающимися Программы. Реализация программы «Кибербезопасность» предусматривает входную диагностику, текущий контроль, промежуточную и итоговую аттестацию обучающихся.

Входная диагностика осуществляется в форме опроса, позволяющего оценить мотивацию к обучению. Текущий контроль включает формы: опрос, тестирование по изучаемым темам, проведение практических/лабораторных работ. Тестирование осуществляется в системе NetAcad Сетевой академии Cisco (https://www.netacad.com). Промежуточная аттестация проводится в форме тестирования. Итоговая аттестация проводится в форме итогового зачета.

Формы проведения аттестации:

- выполнение практических/лабораторных работ;

- тестирование;
- зачет;
- опрос.

Средства контроля

Контроль освоения обучающимися программы осуществляется в процессе оценивания следующих параметров:

- результаты тестирования;
- результаты лабораторной работы.

Результативность обучения дифференцируется по трем уровням: низкий, средний, высокий.

Оцениваемые показатели	***Высокий уровень***	***Средний уровень***	***Низкий уровень***
Знание основных понятий по специальности кибербезопасность	Обучающийся отлично знает основные понятия и свободно ими оперирует	Обучающийся хорошо знает основные понятия и оперирует ими без ощутимых затруднений	Обучающийся не уверенно знает основные понятия и не может ими оперировать
Знание основных понятий в следующих разделах: - базовые понятия кибербезопасности; - специальность в сфере кибербезопасности и юридические аспекты работы с данными; - архитектура систем хранения данных и обеспечение их безопасности; - существующие угрозы, уязвимости систем и методы атак; - способы защиты информации, методы шифрования данных; - обеспечение	Обучающийся знает и уверенно отвечает на вопросы по следующим разделам: - базовые понятия кибербезопасности; - специальность в сфере кибербезопасности и юридические аспекты работы с данными; - архитектура систем хранения данных и обеспечение их безопасности; - существующие угрозы, уязвимости систем и методы атак; - способы защиты информации, методы шифрования данных;	Обучающийся удовлетворительно знает и с небольшой помощью педагога отвечает на вопросы по следующим разделам: - базовые понятия кибербезопасности; - специальность в сфере кибербезопасности и юридические аспекты работы с данными; - существующие угрозы, уязвимости систем и методы атак; - способы защиты информации, методы шифрования данных	Обучающийся неуверенно отвечает на вопросы по следующим разделам: - базовые понятия кибербезопасности; - специальность в сфере кибербезопасности и юридические аспекты работы с данными; - способы защиты информации, методы шифрования данных; - обеспечение целостности данных

целостности данных; - защита по уровням доступа к информации	- обеспечение целостности данных; - защита по уровням доступа к информации		
Практические умения и навыки	Обучающийся уверенно и самостоятельно применяет полученные знания: - по защите персональных данных; - алгоритмам шифрования; - хеш-функции; - взлому хеша; - стратегиям разграничения доступа к данным; - обеспечению доступности через резервирование компонентов сети; - повышению надежности оборудования	Обучающийся применяет полученные знания: - по защите персональных данных; - алгоритмам шифрования; - стратегиям разграничения доступа к данным; - обеспечению доступности через резервирование компонентов сети; - повышению надежности оборудования	Обучающийся применяет полученные знания: - по защите персональных данных; - алгоритмам шифрования; - стратегиям разграничения доступа к данным; - повышению надежности оборудования

ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

Учебно-методические условия реализации программы

При реализации данной Программы основными формами проведения занятий являются комбинированные занятия, состоящие из теоретической и практической части.

Усвоение материала контролируется при помощи тестирования и выполнения практических/лабораторных работ.

Итоговое занятие объединения проводится в форме зачетной работы.

Программа может быть реализована с использованием систем дистанционного обучения, лекционных и практических материалов Сетевой Академии CISCO, представленных в рамках курса Cybersecurity Essetials.

Материально-технические условия реализации Программы

Продуктивность работы во многом зависит от качества материально-технического оснащения процесса. Программа реализуется в аудитории

образовательной организации с применением технических средств обучения:

<u>инфраструктура организации:</u>

- учебный кабинет;

<u>технические средства обучения:</u>

- компьютеры с характеристиками, не уступающим Intel Core i5, объемом оперативной памяти от 8 Gb, дисковой памяти не менее 500 GB, объединенных в локальную вычислительную сеть с выделенным сервером домена;
- проектор;
- экран;
- принтер;
- сканер;
- ПО Cisco Packet Tracer, Oracle VM VirtualBox, последние версии наиболее распространённых интернет-браузеров (Google Chrome, Mozilla Firefox) с поддержкой Flash и Java.

СПИСОК ЛИТЕРАТУРЫ, ИСПОЛЬЗУЕМОЙ ПРИ НАПИСАНИИ ПРОГРАММЫ

1. Адаменко М. Основы классической криптологии. Секреты шифров и кодов. – Москва: ДМК Пресс, 2017.
2. Белоус А. И., Солодуха В.А. Кибероружие и кибербезопасность. О сложных вещах простыми словами. – Москва: Инфра-Инженерия, 2020.
3. Белоус А.И., Солодуха В.А. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения. – Москва: ТЕХНОСФЕРА, 2021.
4. Деза Е.И., Котова Л.В. Введение в криптографию: Теоретико-числовые основы защиты информации. – Санкт-Петербург: Ленанд, 2021.
5. Диогенез Ю., Озкайя Э. Кибербезопасность: стратегии атак и обороны. / Перевод Д.А. Беликова. – Москва: ДМК Пресс, 2020.
6. Камский В.А. Защита личной информации в интернете, смартфоне и компьютере. – Москва: Наука и Техника, 2017.
7. Колисниченко Д.Н. Секреты безопасности и анонимности в Интернете. – Санкт-Петербург: БХВ-Петербург, 2020.
8. Кренин А., Колисниченко Д., Самоучитель системного администратора. – Санкт-Петербург: БХВ-Петербург, 2019.

9. Лаврова Д.С. Математические методы обнаружения и предотвращения компьютерных атак на крупномасштабные системы. – Москва: Горячая линия – Телеком, 2019.

10. Мартиросян А. Формирование системы обеспечения безопасности киберпространства. Монография. – Москва: Проспект, 2022.

11. Масалков А.С. Особенности киберпреступлений. Инструменты нападения и защита информации. – Москва: ДМК Пресс, 2018.

12. Овчинский В. Основы борьбы с киберпреступностью и кибертерроризмом. Хрестоматия. – Москва: Норма, 2017.

13. Сафронов Е. В. Азы кибергигиены. Методологические и правовые аспекты. – Москва: Проспект, 2018.

14. Торстейнсон П., Ганеш Дж.Г.А. Криптография и безопасность втехнологии .NET. – Москва: Лаборатория знаний, 2018.

15. Шелупанов А.А., Смолина А.Р. Форензика. Теория и практика расследования киберпреступлений. – Москва: Горячая линия – Телеком, 2019.

16. Ярошенко А. Хакинг на Android. – Москва: Наука и Техника, 2022.

17. Ярошенко А. В. ХАКИНГ на примерах. Уязвимости, взлом, защита.
– Москва: Наука и Техника, 2021.

18. IT как оружие. Какие опасности таит в себе развитие высоких технологий. – Санкт-Петербург: Альпина Паблишер, 2020.

19. Курс Сетевой Академии в сфере кибербезопасности [Электронный ресурс] // сайт: Networking Akademy Cisco. URL: https://www.netacad.com/courses/security/cybersecurity-essentials
(Датаобращения 01.02.2022).