РУКОН ЦЕЛЬ
МНОГОПРОФИЛЬНЫЙ ЦЕНТР КВАЛИФИКАЦИЙ

Автономная некоммерческая организация
дополнительного профессионального образования
«Многопрофильный центр квалификаций «Цель»

УТВЕРЖДАЮ
Директор АНО ДПО «МЦК «Цель»

О. В. Самохарова

Приказ №4п/2023-БО
от «12» апреля 2023 г.

Одобрена на заседании
педагогического совета
Протокол №3 от «03» апреля 2023 г.

Дополнительная общеобразовательная
общеразвивающая программа
для взрослых

«ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ»

(5 акад. час.)

Автор-составитель:
Сойманова Светлана Викторовна, методист

г. Санкт-Петербург, 2023 г.

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Дополнительная общеобразовательная общеразвивающая программа «Основы кибербезопасности» АНО ДПО «МЦК «Цель» (далее – Программа) имеет техническую направленность.

1.1. Нормативно-правовую основу разработки Программы составляют:

- Конституция Российской Федерации;
- Федеральный закон "Об образовании в Российской Федерации" от 29.12.2012 N 273-ФЗ;
- Приказ Министерства просвещения РФ от 27 июля 2022 г. N 629 "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам";
- Приказ Минобрнауки России от 23.08.2017 N 816 "Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ";
- Постановление Главного государственного санитарного врача Российской Федерации от 28.09.2020 г. № 28 «Об утверждении санитарных правил СП 2.4. 3648-20 «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи»;
- Постановление Главного государственного санитарного врача РФ от 28.01.2021 N 2 "Об утверждении санитарных правил и норм СанПиН 1.2.3685-21 "Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания";
- Методические рекомендации по проектированию дополнительных общеразвивающих программ (включая разноуровневые программы) (Приложение к письму Департамента государственной политики

в сфере воспитания детей и молодежи Министерства образования и науки РФ от 18.11.2015 № 09-3242);

- Устав Автономной некоммерческой организации дополнительного профессионального образования «Многопрофильный центр квалификаций «Цель».

1.2. Актуальность программы

В современном мире информационная безопасность является одной из самых актуальных и важных тем. Все больше людей используют интернет для своих повседневных задач, а также для работы и учебы. С одной стороны, это дает огромные возможности для получения знаний и общения с людьми со всего мира. С другой стороны, в интернете есть множество угроз и опасностей, таких как вирусы, хакеры, мошенничество и многие другие.

Изучение навыков компьютерной безопасности важно для учащихся по многим причинам:

1. Защита личной информации. В цифровую эпоху все больше личной информации о людях хранится в цифровом формате. Злоумышленники могут использовать эту информацию для мошенничества, кражи личности и других преступлений. Изучение навыков компьютерной безопасности поможет старшеклассникам защитить свою личную информацию и избежать негативных последствий.

2. Защита компьютерных систем. Компьютерные системы используются в различных областях, и их защита очень важна. Учащиеся могут изучать навыки компьютерной безопасности, чтобы защитить компьютерные системы своей школы, колледжа или университета от вредоносных программ и кибератак.

3. Карьерные возможности. Навыки компьютерной безопасности являются очень востребованными на рынке труда, и изучение их может помочь учащимся получить конкурентные преимущества при поступлении в университет или при поиске работы в области технологий.

4. Понимание технологического мира. Сегодня технологии окружают нас повсюду, и понимание, как они работают, может быть полезным для жизни и карьеры старшеклассников. Изучение навыков компьютерной безопасности поможет им понять, как работают различные программы и как они могут быть защищены от вредоносных программ и кибератак.

В целом, изучение навыков компьютерной безопасности может быть полезным для учащихся в различных аспектах их жизни, от личной безопасности до карьерных возможностей.

1.3. Новизна программы

Все знают правила поведения в интернете и за компьютером. О том что нельзя переходить на подозрительные сайты, открывать письма от неизвестных отправителей, иметь на своем рабочем компьютере и телефоне антивирус. Но никто, никогда не объяснял почему нужно вести себя именно так. Мы говорим “Вирус”, но не понимаем как он работает, говорим хакер, но не знаем кто это и чем именно занимается. На данном курсе мы не только расскажем о методах противодействия хакерским атакам, интернет-мошенникам и вредоносному программному обеспечению, но и покажем как происходит хакерская атака на сайт, как злоумышленник ищет уязвимости в обороне сайта и как пользуется в полученной информацией, как работает вирус и чем он в действительности опасен. Курс расскажет не только о том как определить зараженные или вредоносные ресурсы в сети интернет, но что делать, если вы все таки на них попали. В рамках данного курса будет развенчан романтический образ хакеров и показан реальный ущерб от действий хакеров.

1.4. Отличительные особенности программы

Отличительными особенностями данной программы является ориентированность на практическое подтверждение доводимой до учащихся информации. Все что учащиеся увидят в рамках данного курса будет

подкреплено реальными живыми примерами. Также данный курс покажет реальный ущерб от хакерских атак и противоправных действий в области информационной безопасности, разрушающий миф о романтизме хакерства. В процессе обучения учащиеся узнают о том, как неосмотрительные действия пользователя при использовании устройств и сети интернет могут повлиять не только него самого, но и на окружающих.

Преподаватели курса являются действующими специалистами ведущих компаний страны в области информационной безопасности. Они имеют огромный опыт и возможность продемонстрировать тот или иной пример с различных точек зрения. Благодаря этому примеры, демонстрируемые преподавателями, становятся более понятными и живыми, что повышает интерес обучающихся к занятиям.

1.5. Цель программы

Знакомство учащегося с потенциальными угрозами при использовании современного программного обеспечения и сети интернет, способами их выявления и устранения при использовании информационных систем.

1.6. Задачи программы

- формирование навыков по оценке уязвимости компьютерных сервисов;

- знакомство с методами и инструменты киберзащиты.

- формирование навыков по поиску и выделению необходимой информации, структурированию знаний, самостоятельному созданию алгоритмов деятельности при решении проблем творческого и поискового характера);

- формирование коммуникативных навыков;

- формирование навыков коллективной работы учащихся;

1.7. Планируемые результаты обучения

В результате освоения программы, учащиеся будут обладать набором определенных компетенций:

- у учащихся будет сформирована система знаний в области анализа и оценки уязвимости компьютерных сервисов;

- учащиеся приобретут знания методики киберзащиты и освоят инструменты по предотвращению компьютерных угроз.

- у учащихся разовьется творческий потенциал;

- учащиеся научатся анализировать, логически и образно мыслить;

- у учащихся сформируются навыки коллективной работы.

1.8. Содержание Программы представлено общей характеристикой, учебным планом, календарным учебным графиком, содержанием тем, планируемыми результатами освоения Программы, условиями реализации и системой оценки результатов освоения Программы.

1.9. Категория обучающихся

Программа рассчитана на взрослых обучающихся.

1.10. Форма обучения: очно-заочная с применением электронного обучения и дистанционных образовательных технологий

1.11. Режим занятий

Учебная нагрузка по программе составляет не более 5 учебных занятий в неделю. Продолжительность занятия –40 минут. Занятия проводятся по группам, подгруппам или индивидуально.

1.12. Трудоемкость программы

Нормативная трудоемкость обучения по Программе – 5 академических часов, включая все виды аудиторной и внеаудиторной учебной работы учащихся.

1.13. Форма документа, выдаваемого по результатам освоения программы

По результатам освоения программы учащимся выдается сертификат о прохождении обучения установленного образовательной организацией образца.

2. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1. УЧЕБНЫЙ ПЛАН ДОПОЛНИТЕЛЬНОЙ ОБЩЕОБРАЗОВАТЕЛЬНОЙ ОБЩЕРАЗВИВАЮЩЕЙ ПРОГРАММЫ

«Основы кибербезопасности»

№ п/п	Наименование тем	Количество часов (ак.час)				Формы аттестации/ контроля
		Всего	Теория	Практика	Самостоятельная работа	
1	*2*	*3*	*4*	*5*	*6*	*7*
1.	Противодействие хакерским атакам	1	1	-	-	Опрос
2.	Защита сайта от взлома	1	1	-	-	Опрос
3.	Безопасность личных данных	1	1	-	-	Опрос
4.	Доступные методы и инструменты киберзащиты	1	1	-	-	Опрос
5.	Итоговое тестирование	1	1	-	-	Тест
	Итого часов	5	5	-	-	

2.2. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Наименование тем	Аудиторные занятия	Всего часов
	1 день	
1. Противодействие хакерским атакам	Т1(ДОТ)	1
2. Защита сайта от взлома	Т1(ДОТ)	1
3. Безопасность личных данных	Т1(ДОТ)	1
4. Доступные методы и инструменты киберзащиты	Т1(ДОТ)	1
5. Итоговое тестирование	Т1(ДОТ)	1
Всего часов	5	5

Примечание:

«Т1» - теоретическая подготовка,1 час; «ДОТ» - дистанционные образовательные технологии.

2.3. СОДЕРЖАНИЕ ТЕМ

Тема 1. Противодействие хакерским атакам (1 час)

Теория. Методы и способы цели хакерских атак. Влияние хакерских атак на общество. Потенциальные жертвы хакеров и возможные последствия. Развенчание романтического образа хакера. Невольные соучастники хакерских атак. Как не стать соучастником выгоды хакерских атак, риски и последствия в результате неудачи. Сравнение выгод и рисков.

Тема 2. Защита сайта от взлома (1 час)

Теория. Демонстрация реального взлома демонстрационного сайта. Основные методы и подходы к взлому сайтов. Пострадавшие и последствия. Выстраивание обороны сайта и противодействие атакам. Чек лист проверки сайта на устойчивость к базовым методам взлома.

Тема 3. Безопасность личных данных (1 час)

Теория. Какие данные необходимо защищать. Как "утекают" личные данные. Способы использования личных данных. Влияние утечки ваших личных на окружающих. Как защитить свои личные данные и окружающих.

Тема 4. Доступные методы и инструменты киберзащиты (1час)

Теория. Демонстрация ошибочных действий пользователя при взаимодействии с компьютером и в сети интернет. Демонстрация последствий таких действий для себя и окружающих. Демонстрация скорости подбора паролей в зависимости от требований к их сложности. Как без навыков программирования распознать потенциально вредоносный сервис. Что делать если вы уже использовали вредоносный сервис.

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

3.1. МАТЕРИАЛЬНО – ТЕХНИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

С целью реализации Программы с применением исключительно электронного обучения, дистанционных образовательных технологий в образовательной организации созданы условия для функционирования электронной информационно-образовательной среды, включающей в себя электронные информационные ресурсы, электронные образовательные ресурсы, совокупность информационных технологий, телекоммуникационных технологий, соответствующих технологических средств и обеспечивающей освоение обучающимися образовательных программ в полном объеме независимо от места нахождения обучающихся.

Требуемое оборудование

Каждому участнику образовательного процесса необходимо иметь персональный компьютер с доступом в сеть Интернет.

Требуемое программное обеспечение (для учащихся)

Рекомендовано: браузер Google Chrome, ОС Windows, текстовый редактор MS Word, электронные таблицы MS Excel.

Наименование систем, ресурсов, программ, оборудования, используемых в образовательном процессе

1. ***Информационно-коммуникационные системы:***

- Операционная система: Windows 10 (или выше);
- Среда виртуализации VirtualBox;
- браузер Google Chrome.

2. ***Система дистанционного обучения (СДО):***

- Вебинар.Ру.

3.2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММЫ (ЛИТЕРАТУРА)

Учебно-методическое обеспечение учебного процесса с применением электронного обучения, дистанционных образовательных технологий включает электронные информационные образовательные ресурсы (ЭИОР), размещенные на электронных носителях и/или в электронной среде поддержки обучения.

№ п/п	Наименование темы	Перечень электронных информационных ресурсов (электронно-библиотечных ресурсов и систем, информационно-справочных систем)	Перечень электронных образовательных ресурсов
1.	Противодействие хакерским атакам	Центр кибербезопасности https://www.cert.ru/ Журнал "Хакер" https://xakep.ru/ Центр обеспечения безопасности информации "Лаборатория Касперского" https://www.kaspersky.ru/ Блог о кибербезопасности "Habr" https://habr.com/ru/hub/security/ Электронный ресурс "Infosecurity" https://www.infosecurity-magazine.ru/	CybersecurityPro.ru - https://cybersecuritypro.ru/ Хакер.ру - https://xaker.ru/ InfosecurityRussia.ru - https://www.infosecurityrussia.ru/ SecNews.ru - https://www.secnews.ru/ SecurityLab.ru - https://www.securitylab.ru/
2.	Защита сайта от взлома	Центр кибербезопасности https://www.cert.ru/ Журнал "Хакер" https://xakep.ru/ Электронный ресурс "SecurityLab" https://www.securitylab.ru/ Блог о кибербезопасности "Habr" https://habr.com/ru/hub/security/	Habr.com - https://habr.com/ru/hub/infosecurity/ WebSecurify.ru - https://websecurify.ru/ InfosecurityRussia.ru - https://www.infosecurityrussia.ru/ SecurityLab.ru - https://www.securitylab.ru/ Pentestit.ru - https://pentestit.ru/
3.	Безопасность личных	Федеральная служба по надзору в сфере связи,	Информационно-образовательный портал

	данных	информационных технологий и массовых коммуникаций (Роскомнадзор) https://rkn.gov.ru/ Российский центр кибернетической безопасности https://www.cybersafety.ru/ Блог о кибербезопасности "Habr" https://habr.com/ru/hub/security/ Центр кибербезопасности https://www.cert.ru/ Электронный ресурс "Infosecurity" https://www.infosecurity-magazine.ru/	"Безопасность в Интернете": https://safeinternet.ru/ Портал "Кибербезопасность для всех": https://cybersecurity.ru/ Информационно-образовательный портал "Безопасный интернет": https://bezopasnost.ru/ Портал "Личные данные": https://personaldata.ru/ Интернет-школа "Кибермозг": https://cyberbrain.ru/ Интернет-школа "Безопасный интернет": https://bezopasny-internet.ru/ Портал "Кибершкола": https://cyberschool.online/ Информационно-образовательный портал "Безопасность в интернете": https://bezopasnostvinternet.ru/
4.	Доступные методы и инструменты киберзащиты	Журнал "Хакер" https://xakep.ru/ Центр кибербезопасности https://www.cert.ru/ Российский центр кибернетической безопасности https://www.cybersafety.ru/ Электронный ресурс "SecurityLab" https://www.securitylab.ru/ Блог о кибербезопасности "Habr" https://habr.com/ru/hub/security/	Портал «Кибербезопасность для всех» - https://cyber-dojo.ru/ Портал «Центр киберзащиты» - https://cybercenter.ru/ Портал «Информационная безопасность» - https://www.securitylab.ru/ Портал «Интернет безопасность» - https://www.internet-security.ru/ Портал «Безопасность в интернете» - https://bezopasnost.ru/ Портал «Киберзащита» - https://cyber-sec.pro/ Портал «Угрозы в интернете» - https://www.securitylab.ru/threats/ Портал «Анализ безопасности» - https://pentestit.ru/ Портал «Be Wary» - https://bewary.pro/ Портал «Информационная безопасность для бизнеса» - https://www.cisoconnect.com/

Примечание:

Перечень учебной литературы определяется образовательным учреждением. Список рекомендуемой литературы представлен в Приложении 3.

3.3. ИНФОРМАЦИОННО-МЕТОДИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ВКЛЮЧАЮТ:

1. учебный план;
2. календарный учебный график;
3. образовательную программу;
4. методические материалы и разработки;
5. расписание занятий.

3.4. КАДРОВОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММЫ

Педагогическая деятельность по реализации Программы осуществляется лицами, имеющими среднее профессиональное или высшее образование (в том числе по направлению, соответствующему направлению дополнительной общеобразовательной программы) и отвечающим требованиям профессионального стандарта "Педагог дополнительного образования детей и взрослых", утвержденного приказом Минтруда России от 5 мая 2018 г. N 298н.

Персональный состав педагогических работников, обеспечивающих реализацию образовательного процесса, отражен в Приложении 2.

4. ОБЩИЕ ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Обучение по программе осуществляется в очно-заочной форме с применением электронного обучения и дистанционных образовательных технологий.

Образовательный процесс осуществляется в режиме онлайн, в форме вебинаров.

Образовательная деятельность учащихся предусматривает следующий вид учебных занятий: лекции, определенные учебным планом.

При реализации Программы используются различные образовательные технологии во время проведения аудиторных (онлайн) занятий: технология «перевернутого класса», геймификация, кейс-технология, онлайн-конференция и т.д.

5. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

Оценка качества освоения программы осуществляется в виде текущего контроля знаний обучающихся, итогового тестирования.

Текущий контроль знаний осуществляется преподавателем в форме опроса. Перечень вопросов текущего контроля знаний обучающихся представлен в Приложении 1.

Итоговое тестирование состоит из 10 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала. (Приложение 1).

Критерии оценки результатов выполнения итогового тестирования

По результатам прохождения итогового тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев:

отметка «зачтено» – 30% и более правильных ответов;

отметка «не зачтено» – менее 30% правильных ответов.

Приложение 1

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Примеры вопросов текущего контроля знаний

1. Что такое кибербезопасность и зачем она нужна?
2. Что такое хакерство и какие существуют виды хакерских атак?
3. Какие виды киберугроз существуют?
4. Что такое вирусы и как они распространяются?
5. Какие есть способы защиты своего компьютера от вирусов?
6. Что такое "фишинг" и как от него защититься?
7. Какие есть способы создания надежного пароля?
8. Какие существуют методы шифрования данных и зачем они нужны?
9. Что такое двухфакторная аутентификация и как она работает?
10. Какие есть основные правила безопасности при работе в интернете?
11. Что делать, если ваша учетная запись была взломана?
12. Какие есть программы для обнаружения и удаления вирусов?
13. Как работает защита сайтов от взлома и какие меры безопасности нужно принимать при создании сайта?
14. Какие есть виды атак на сайты и как от них защититься?
15. Что такое "бэкап" и зачем он нужен для защиты данных?

Примеры вопросов итогового тестирования

1. Какого типа тестирования безопасности приложений не существует?

1. Black-box
2. White-box
3. Red-box
4. Grey-box

2. В чем заключаются task-based CTF соревнования?

1. Противостояние команд Red Cell (взломщиков) и Blue Cell (защитников)
2. Поиск флага в процессе заданий на хакинг
3. Проведение тестирования безопасности реальных систем
4. Анализ веб-приложения на уязвимости

3. Как называется атака перебора пароля по словарю?

1. Bug bounty
2. Фаззинг
3. Brute-force
4. XSS

4. Какое средство защиты чаще всего используют для веб-приложений?

1. Web Application Firewall
2. Web Scanner
3. Host-based Firewall
4. Vulnerability Scanner

5. Какой категории персональных данных не существует?

1. Общедоступные
2. Иные
3. Личные
4. Биометрические

6. Какой инструмент используется для перехвата и анализа трафика в сети?

1. Burp Suite Intruder
2. Burp Suite Repeater
3. Wireshark
4. Hydra

7. Главный документ, определяющий законодательство в сфере ПДн в Российской Федерации?

1. Постановление Правительства №1119
2. Федеральный закон №152
3. Приказ ФСТЭК №21
4. Федеральный закон №149

8. Что такое хеш пароля?

1. Значение, зависимое от логина и пароля вместе
2. Результат взлома пароля
3. Строка, применяемая для авторизации вместо пароля
4. Набор символов после применения к паролю математической функции

9. Зачем нужен SSL-сертификат сайта?

1. Для шифрования подключений
2. Для подтверждения подлинности сайта
3. Для использования средств защиты
4. Для удаленного подключения к серверу

10. Выставите в верном порядке приведенные пароли от самого безопасного (1) до самого небезопасного (4). (Пример ответа - abcd)

1. $p0ngeB0b
2. SecurePassworD
3. lJ6SFg1wc5
4. K6%7NZ#EQh^*EZ8

РУКОН ЦЕЛЬ
МНОГОПРОФИЛЬНЫЙ ЦЕНТР КВАЛИФИКАЦИЙ

Приложение 2

ПЕРСОНАЛЬНЫЙ СОСТАВ ПЕДАГОГИЧЕСКИХ РАБОТНИКОВ

№ п/п	ФИО	Занимаемая должность	Сведения об уровне образования	Квалификация	Наименование направления подготовки и (или) специальности	Сведения об имеющихся: ученой степени, ученом звании	Сведения о повышении квалификации и (или) профессиональной переподготовке	Общий стаж работы	Стаж работы по специальности	Преподаваемые темы
1.	Почаевец Андрей Андреевич	Программный директор АНО ДПО МЦК "Цель", преподаватель линейки программ 1С	Высшее профессиональное; Среднее профессиональное	Инженер; Техник	Информационные системы и технологии Программное обеспечение вычислительной техники и автоматизированных систем	-	2021 Luxoft training Luxoft training, REQ-065 Управление требованиями в Agile; 2020 Первый Бит Первый Бит, Управленческий учет в "1С:Зарплата и управление персоналом КОРП"; 2020 Первый Бит Первый Бит, Кадровый учет в "1С:Зарплата и управление персоналом 3.1"; 2020 ИнфоСтарт	19 лет	1 год	Тема 2

							ИнфоСтарт, DevOps для 1С			
2.	Бердашкевич Артём Эдуардович	Генеральный директор ИТ-компании “Tiger- Tag”	Высшее	Магистр	Информационная безопасность	-	Анализ рисков информационной безопасности предприятия. Безопасность IoT устройств. Построение защищенных информационных систем. Этичный хаккинг и тестирование на проникновение	6 лет	1 год	Тема 1
3.	Лукьянцев Игорь Сергеевич	Специалист по информационной безопасности	Среднее профессиональное	Техник-программист	Программирование в компьютерных системах	-	-	2 года	2 года	Тема 3
4.	Яицкий Антон Андреевич	Специалист по информационной безопасности	Высшее	Магистр	Информационная безопасность	-	Администрирование ОС Astra Linux: Расширенное администрирование - РусБИТех-Астра QA School - Digital Design; Программирование и автоматизация	1 год	1 год	Тема 4

							Python - повышение квалификации Университет ИТМО			

Приложение 3

СПИСОК ЛИТЕРАТУРЫ

Литература для педагога

1. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. Учебное пособие. Студентам ССУЗов, Форум, 2023, 416 стр.

2. Глушаков С.В., ТесленкоН.С., Бабенко М.И.: Секреты хакера: защита и атака, АСТ, 2008, 544 стр.

3. Джоел Скембрей, Шема Майк, Секреты хакеров. Безопасность Web-приложений - готовые решения, *Издательский дом "Вильямс», Москва, 2003, 384 стр.*

4. Малюк А.А., Защита информации в информационном обществе. Учебное пособие для вузов, Горячая Линия - Телеком, 2020, 230 стр.

5. Бабаш А.В., Баранова Е.К. Основы информационной безопасности. Учебник. Студентам ССУЗов, РИОР, 2022, 202 стр.

Литература для обучающихся

1. Маккарти Б. Кибердзюцу: кибербезопасность для современных ниндзя, Питер, 2022, 224 стр.

2. Диогенес Ю., Озкайя Э., Кибербезопасность. Стратегии атак и обороны, ДМК Пресс, 2020, 326 стр.

3. Коллинз М., Защита сетей. Подход на основе анализа данных, ДМК Пресс, 2020, 308 стр.

4. Ломакин П., Шрейн Д., Антихакинг, Майор, 2002, 512 стр.

5. Бирюков А.А. Информационная безопасность: защита и нападение, ДМК Пресс, 2007, 536 стр.

6. Фленов М.Е., Web-сервер глазами хакера. 3-е изд., перераб.и доп, БХВ, 2021, 256 стр.