ООО «АНТКОЛОНИ»

УТВЕРЖДЕНА

Приказ № 2

от «11» февраля 2024 г.

Левин М.В.

Дополнительная общеразвивающая программа

«Основы кибербезопасности»

Возраст учащихся: от 18 лет

Срок реализации программы: 5 дней

Разработчик:

Левин М.В.

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1.1. Направленность программы

Дополнительная общеобразовательная программа «Основы кибербезопасности» имеет техническую направленность.

Повсеместное использование информационных систем и технологий для обеспечения работы предприятий и организаций диктует необходимость в организации их кибербезопасности (информационной безопасности) от атак и прочих злонамеренных действий в информационной среде.

1.2 Актуальность программы

Актуальность программы обусловлена, во-первых, тем фактом, что инженерам и специалистам, работающим в сфере кибербезопасности, необходимо сформировать общее представление о всех направлениях деятельности отрасли с практической точки зрения.

Во-вторых, данная образовательная программа является базовой, и тематически и практически связана с другими образовательными программами, предлагаемыми компанией, направленными на получение знаний и формирование навыков, необходимых отрасли.

1.2. Отличительные особенности программы

Программой предусмотрена онлайн форма обучения, посредством собственной образовательной платформы с уникальной лабораторной базой.

Учащимся, успешно освоившим программу, выдается сертификат установленного образца.

1.3. Адресат программы

Программа предназначена для людей, начинающих знакомиться с кибербезопасностью, а также инженерам, желающим систематизировать свои знания в этой области.

1.4. Объём и срок реализации программы

Дополнительная общеобразовательная общеразвивающая программа рассчитана на 5 дней обучения в количестве 40 учебных часов, необходимых для освоения данной программы.

Режим занятий: 5 занятий в неделю по 8 часов (2 теоретических занятия и 2 занятия, направленных на закрепление пройденного материала).

Учебная нагрузка по видам деятельности:

Продолжительность теоретического занятия – 2 часа. Продолжительность практического занятия – 2 часа

Общая трудоемкость программы – 40 часов.

1.5. Цель и задачи программы

Цель программы – позволить слушателям изучить основы кибербезопасности: направления и сегменты деятельности этой

технологической отрасли, классы и типы её продуктов, технологии и методики их использования. Программа построена на принципе, согласно которому кибербезопасность – это, прежде всего, процесс, поэтому большое внимание уделяется тому, как именно выстроить процессы кибербезопасности корпоративного уровня в рамках её единой архитектуры.

В процессе обучения решаются следующие **задачи**:

1.Определение уровня знаний учащегося;

2.Ознакомление учащегося с архитектурой кибербезопасности;

3.Подготовка учащегося к практической деятельности в данной отрасли;

4.Обеспечение учащегося знаниями, достаточными проектирования внедрения основных технологий и процессов кибербезопасности в корпоративной инфраструктуре.

1.6. Условия реализации программы

К реализации программы привлекаются специалисты с профильным образованием в области кибербезопасности, а также с опытом работы в ведущих отечественным и мировых компаниях, решающих вопросы кибербезопасности.

Занятия проводятся с помощью собственной онлайн-платформы с доступом к лабораторным стендам, имитирующим настоящую корпоративную инфраструктуру.

1.7. Планируемые результаты

В результате освоения данной дополнительной общеобразовательной общеразвивающей программы учащийся получит новые и усовершенствует имеющиеся навыки и умения:

– навыки проектирования архитектуры корпоративной кибербезопасности;

– умение настраивать средства фильтрации трафика;

– умение настраивать средства защиты электронной почты;

– умение обрабатывать статистическую информацию в области кибербезопасности ;

– умение проводить аудит кибербезопасности;

– знания в области моделирования угроз кибербезопасности.

2. УЧЕБНЫЙ ПЛАН

Модуль ТБУ/А2 (базовый уровень)

№ п/п	Название раздела, темы	Количество часов			Формы контроля
		Всего	Теория	Практика	
1	2	3	4	5	8
1.	Тема «Критерии защищенности информации»	4	2	2	–
2.	Тема «Моделирование	4	2	2	–

	угроз и оценка рисков кибербезопасности»				
3.	Тема «Безопасность сетей TCP/IP»	4	2	2	–
4.	Тема «Криптография и VPN»	4	2	2	–
5.	Тема «Безопасность операционных систем»	4	2	2	–
6.	Тема «Безопасность приложений»	4	2	2	–
7.	Тема «Безопасность индустриальных объектов»	4	2	2	–
8.	Тема «Кибербезопасность информации»	4	2	2	–
9.	Тема «Операционная кибербезопасность»	4	2	2	–
10.	Тема «Проектирование и управление кибербезопасность/»	4	2	2	–
	Итоговая аттестация	–	–	–	**-**
	Итого:	**40**	20	20	

3. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Дата начала обучения по программе	**Дата окончания обучения по программе**	**Всего учебных дней**	**Количество учебных часов**	**Режим занятий**
утверждается организацией после набора учащихся	утверждается организацией после набора учащихся	**5**	**40**	4 занятия в неделю по 2 часа (2 теоретических занятия и 2 занятия, направленных на закрепление пройденного материала)

СОДЕРЖАНИЕ ПРОГРАММЫ

к дополнительной общеобразовательной программе
«Основы кибербезопасности

Возраст учащихся: от 18 лет

Срок реализации программы: 5 дней

Разработчик:
Левин М.В.

Содержание программы

- Тема 1 – Критерии защищенности информации.
  - Конфиденциальность, целостность, доступность.
  - Контроль доступа и его типы.
  - Механизмы контроля доступа.
  - Архитектура корпоративной кибербезопасности.

- Тема 2 – Моделирование угроз и оценка рисков кибербезопасности.
  - Методики моделирования угроз.
  - Методики оценки и управления рисками.
  - Построение процессов и архитектуры кибербезопасности на основе модели угроз.

- Тема 3 – Безопасность сетей TCP/IP.
  - Функциональная классификация механизмов защиты TCP/IP сетей.
  - Контроль доступа к локальной сети. Защита от ARP и DHCP атак.
  - Контроль доступа к локальной сети. 802.1x.
  - Репутационная аналитика. IP, DNS и URL фильтрация.
  - Фильтрация сетевого трафика. Firewall и IPS.
  - Защита от DoS и DDoS атак.
  - Защита Wi-Fi сетей.

- Тема 4 – Криптография и VPN.
  - Принципы шифрования данных.
  - Симметричные шифры.
  - Асимметричные шифры.
  - PKI.
  - Принципы обеспечения целостности данных.
  - Алгоритмы создания MAC.
  - Принципы построения защищенных каналов связи.
  - Принципы работы VPN.
  - Классификация и архитектуры VPN.

- Тема 5 – Безопасность операционных систем.
  - Принципы обеспечения защиты информации внутри ОС.
  - Управление учетными записями.
  - Модели безопасности ОС.
  - Безопасность ОС Windows.
  - Безопасность ОС Linux.
  - Безопасность macOS.
  - Безопасность мобильных ОС.

- Тема 6 – Безопасность приложений.
    - Безопасность Web-приложений.
    - Безопасность электронной почты.
    - Безопасность IP-телефонии.
    - Безопасность облачной инфраструктуры Microsoft365.
    - Безопасность платформ виртуализации.

- Тема 7 – Безопасность индустриальных объектов.
    - Объекты и системы индустриальной инфраструктуры.
    - Компоненты обеспечения кибербезопасности индустриальных объектов
    - Архитектура кибербезопасности индустриальных объектов.

- Тема 8 – Кибербезопасность информации.
    - Работа с персональными данными и приватность информации.
    - Защита от утечек данных.
    - Защита авторского права средствами кибербезопасности.

- Тема 9 – Операционная кибербезопасность.
    - Мониторинг событий и инцидентов кибербезопасности.
    - Реагирование на события и инциденты кибербезопасности.
    - OSINT – Open-Source Intelligence.
    - Threat Intelligence.
    - Анализ уязвимостей.
    - Reverse Engineering вредоносного п/о.
    - Проведение Pentest’а.
    - Цифровая криминалистика.

- Тема 10 – Проектирование и управление кибербезопасностью.
    - Принципы управления кибербезопасностью.
    - Построение процессов управления кибербезопасностью.
    - Политики кибербезопасности.
    - Оценка и метрики работы процессов кибербезопасности.
    - Построение корпоративного SoC’а.

Итоговая аттестация

Выполнение практического задания без заранее подготовленных инструкций.

4. ОЦЕНОЧНЫЕ И МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

4.1. Система контроля результативности обучения

Объектами контроля как обязательного компонента процесса обучения являются приобретаемые учащимися знания и уровень сформированности практических навыков и умений. В процессе освоения учебной программы, предусмотрены **подведение итогов и определение результативности** знаний и умений учащихся (итоговая аттестация).

Формы контроля: итоговая аттестация.

Итоговая аттестация: Итоговая аттестация предполагает выполнение практического задания по проектированию и последующими установкой и настройкой инструментов кибербезопасности в лабораторном стенде. Результат оценивается путем запуска в лабораторной стенде симуляций кибератак: если атаки остановлены настроенными аттестуемым инструментами кибербезопасности – аттестация считается сданной.

4.2. Педагогические методики и технологии, дидактические материалы, информационные источники, используемые при реализации программы

а) основная литература:

1. Никитин В.Н., Юркин Д.В. Протоколы обеспечения безопасности VoIP-телефонии. // Защита информации. Инсайд. 2012. – №3–с.74-81.– 8 с.
2. Никитин В.Н., Юркин Д.В. Оценка вероятностно-временных характеристик защищенной IP-телефонии // Защита информации. Инсайд. 2012. – №4–с.64-71.– 8 с.
3. Никитин В.Н., Ковцур М.М. Пути совершенствования протоколов распределения ключей для IP-телефонии. – СПб.: СПбГУТ, 2013. – 1291 с.
4. Ahmed A., Madani H., Siddiqui T. VoIP Performance Management and Optimization, Rough Cuts. – Cisco Press, 2010. – 448 с.
5. Szigeti T., Hattingh C., Barton R., Briley K. End-to-End QoS Network Design: Quality of Service for Rich-Media & Cloud Networks, 2nd Edition. – Cisco Press, 2014. – 1040 с.
6. Behl A. Securing Cisco IP Telephony Networks. – Cisco Press, 2013. –696 с.

DeLaet G., Schauwers G. Network Security Fundamentals. – Cisco Press, 2005. – 480 с.

7. Bollapragada V., Khalid M., Wainner S. IPSec VPN Design. – Cisco Press, 2005. – 384 с.

8. Convery S. Network Security Architectures. – Cisco Press, 2004. – 792 с.кт-Петербург : Златоуст, 2015.

б) дополнительная литература:

1. Буйневич М. В., Васильева И.Н. Информационная безопасность и защита информации: Учеб. пособие. – СПб.:СПбГИЭУ, 2011. – 175 с.
2. Кириллов Д.И. Пограничный контроллер сессий: настоящее и будущее. – IT эксперт // №11, 2008. – 2 с.

в) другие информационные ресурсы:

1. Профильные web-сайты.