Министерство образования и науки Республики Саха (Якутия)
Государственное бюджетное профессиональное образовательное учреждение
Республики Саха (Якутия) «Покровский колледж»

УТВЕРЖДАЮ
И.о. ГБПОУ РС(Я)
«Покровский колледж»
_____ С.И. Сысолятин
«10» _____ 20_20_г.

Дополнительная профессиональная программа

повышения квалификации

«Кибербезопасность»

г. Покровск, 2020 год

1. Цели реализации программы:

Программа направлена освоение компетенции «Кибербезопасность».

2. Требования к результатам обучения. Планируемые результаты обучения:

Требования к результатам освоения программы

В результате освоения программы обучения слушатель должен приобрести следующие знания и умения, необходимые для качественного изменения компетенций в результате обучения:

Слушатель должен знать:

1. Современные тенденции в области информационных технологий и в подходах к построению ИТ-инфраструктуры;
2. Принципы кибербезопасности, используемые для управления рисками при использовании, обработке, хранении и передаче данных
3. Концепции архитектуры сетевой безопасности, отраслевые стандартны в области анализа, категории инцидентов и разработка контрмер для выявления угроз
4. Методы и приемы, используемые для обнаружения различных видов уязвимостей, средства сбора информации и ее хранения, стратегия использования инструментов кибербезопасности, техники получения несанкционированного доступа и методы прогнозирования угроз.

Слушатель должен уметь:

1. Применять аналитические навыки для диагностики и устранения неисправностей в работе информационных систем и сетей;
2. Анализировать и разрабатывать процедуры интеграции, тестирования, эксплуатации, сопровождения механизмов безопасности информационных систем;
3. Тестировать, внедрять, развертывать, поддерживать и управлять аппаратным и программным обеспечением, а также расследовать, анализировать и реагировать на инциденты кибербезопасности;
4. Собирать, обрабатывать и анализировать оценки угроз кибербезопасности, выявлять и устранять уязвимости.

3. Содержание программы

Категория слушателей: Школьники и студенты

Трудоемкость обучения: 36ч.

Форма обучения: очная.

№	Наименование модулей	Всего, академ. часов	В том числе			Форма контроля
			лекции	практич. занятия	итоговый контроль	
1	2	3	4	5		6
1	Требования охраны труда и техники безопасности при работе с компьютером	*2*	*2*	-	-	-
2	Понятие кибербезопасности	*2*	*2*	-	-	-
3	Виртуализация	*8*	*4*	*4*		
4	Уязвимости системы	*8*	*5*	*3*	-	-
5	Дополнительные возможности	*10*	*4*	*6*	-	-
6	Итоговая аттестация	*6*	-	-	*6*	экзамен
	ИТОГО:	*36*	*17*	*13*	*6*	

3.2.Учебно-тематический план

№	Наименование модулей	Всего, академических часов	В том числе		Форма контроля
			лекции	практические занятия	лекции
1	2	3	4	5	6
1	**Требования охраны труда и техники безопасности при работе с компьютером**	**2**	**2**	-	-
1.1	Требования охраны труда и техники безопасности		1	-	-
1.2	Специфичные требования охраны труда, техники безопасности компетенции		1	-	-
2	**Понятие кибербезопасности**	**2**	**2**	-	-
2.1	Основные термины и понятия кибербезопасности		1	-	-

2.2	Современные технологии анализа безопасности информационных систем		1	-	-
3	**Виртуализация**	**8**	**4**	**4**	-
3.1	Технологии виртуализации		2	2	-
3.2	Oracle VirtualBox.		2	2	-
4	**Уязвимости системы**	**8**	**5**	**3**	-
4.1	Распространенные методы атак и отличительные признаки типовых уязвимостей		3	1	-
4.2	Эксплуатация информационного ресурса		2	2	-
5	**Дополнительные возможности**	**10**	**4**	**6**	-
5.1	Работа с сервером		2	2	-
5.2	Работа с ОС Linux		2	4	-
6	**Итоговая аттестация**	**6**	-	-	**6**
	ИТОГО:	**36**	**17**	**13**	**6**

3.3 Учебная программа

Наименование модулей	Содержание учебного материала
Модуль 1. Требования охраны труда и техники безопасности при работе с компьютером	Тема 1.1. Вредные факторы при работе с компьютерной техникой, их влияние на работоспособность.
	Тема 1.2. Эффективная организация рабочего места при работе с компьютерной техникой.
Модуль 2 Понятие кибербезопасности	Тема 2.1 Основные термины и понятия кибербезопасности.
	Тема 2.2 Современные технологии анализа безопасности информационных систем.
Модуль 3 Виртуализация	Тема 3.1 Технологии виртуализации.
	Тема 3.2 Oracle VirtualBox.
	Практические занятия: Конфигурирование виртуальной машины.
Модуль 4 Поиск уязвимостей	Тема 4.1 Распространенные методы атак и отличительные признаки типовых уязвимостей
	Тема 4.2 Эксплуатация информационного ресурса. Требования к программному обеспечению для

	функционирования информационных ресурсов. Порядок действий при развертывании ПО в требуемой конфигурации.
	Практические занятия: Установка и типовые действия при эксплуатации информационных ресурсов. Отработка навыков поиска уязвимостей веб-сайтов и веб-приложений с использованием специального программного обеспечения.
Модуль 5 Дополнительные возможности	Тема 5.1 Работа с сервером.
	Тема 5.2 Работа с ОС Linux.
	Практические занятия: Занятия по серверам и ОС Linux.
Итоговая аттестация	

3.4. Календарный учебный график (порядок освоения модулей)

Период обучения (дни, недели)*	Наименование раздела, модуля
1 неделя	Модуль 1. Требования охраны труда и техники безопасности Модуль 2. Современные технологии в профессиональной сфере Модуль 3. Виртуализация Модуль 4. Поиск уязвимостей Модуль 5. Дополнительные возможности Итоговая аттестация
Точный порядок реализации разделов, модулей (дисциплин) обучения определяется в расписании занятий.	

4. Материально-технические условия реализации программы

4.1. Для реализации программы учебной дисциплины должны быть предусмотрены следующие специальные помещения:

Мастерская «Кибербезопасность», оснащенный оборудованием и техническими средствами обучения:

- рабочее место преподавателя ОС Windows 10, не менее 4 ГБ RAM, не менее 4 ГБ свободного места на диске, доступ в Интернет.
- посадочные места обучающихся (по количеству обучающихся);
- учебные наглядные пособия;
- комплект учебников (учебных пособий) по количеству обучающихся;
- лицензионное программное обеспечение;
- сервер.

Оборудование, оснащение рабочих мест, инструменты и расходные материалы, необходимые для освоения программы.

5. Учебно-методическое обеспечение программы

1. Техническая документация по компетенции «Кибербезопасность»;
2. Печатные раздаточные материалы для слушателей;
3. Профильная литература.

	Авторы	Заглавие	Издательство, год	Эл. адрес
Л1.1	Фомин Д.В.	Информационная безопасность [Электронный ресурс]: учебно-методическое пособие по дисциплине «Информационная безопасность»	Саратов, 2018	http://www.iprbookshop.ru/77320.html.— ЭБС «IPRbooks»
Л1.2	Фаронов А.Е.	Основы информационной безопасности при работе на компьютере [Электронный ресурс]	М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016	http://www.iprbookshop.ru/52160.html.— ЭБС «IPRbooks»
Л1.3	Аверченков В.И.	Аудит информационной безопасности [Электронный ресурс]: учебное пособие	Брянск: Брянский государственный технический университет, 2012	http://www.iprbookshop.ru/6991.html.— ЭБС «IPRbooks»
3.1. Дополнительная литература				
	Авторы	Заглавие	Издательство, год	Эл. адрес
Л2.1	Рафаэль Херцог, Ролан Ма	Настольная книга администратора Debian	ООО «Книга по требованию», 2016	https://losst.ru/wp-content/uploads/2016/08/debian-handbook.pdf
Л2.2	Брайан Уорд	Внутреннее устройство Linux	Питер, 2016	https://consense.com.ua/ru/lib/showbook/how_linux_works
3.2. Перечень информационно-телекоммуникационной сети "Интернет"				
Э1	Блог программистов по Linux https://otus.ru/nest/linux/			
Э2	Инструменты Kali Linux https://kali.tools/			

Э3	Коллекция библиотек https://www.oracle.com/ru/virtualization/technologies/vm/downloads/virtualbox-downloads.html
Э4	Лаборатория линуксоида https://younglinux.info/
Э5	Виртуальная энциклопедия http://rus-linux.net/lib.php?name=/txt/algol.koi
Э6	Официальная документация Oracle VirtualBox https://www.virtualbox.org/wiki/Documentation
Э7	Официальная документация Kali Linux https://www.kali.org/docs/

3.3. Перечень программного обеспечения
Microsoft Office 2014+, Libra Office, Notepad ++, Sublime Text 3, Web Browser - Firefox Developer Edition, Web Browser – Chrome, Adobe Acrobat reader, Oracle VirtualBox + ВМ Kali Linux, ВМ Debian, MS Visual Studio Enterpise, MS Vs code, WebStorm, Репозиторий Debian, Zeal, OpenServer (Ultimate), 7Zip, Windows 7 - 10
3.4. Перечень информационных справочных систем
Электронно-библиотечная система «Университетская библиотека онлайн»: http://biblioclub.ru. Образовательная платформа «Urait»: https://urait.ru/ Электронно-библиотечная система «Лань»: http://e.lanbook.com/ Информационная справочная система: СПС КонсультантПлюс http://www.consultant.ru/ Профессиональные базы данных: 1. Электронная библиотечная система http://elibrary.asu.ru/ 2. Научная электронная библиотека elibrary http://elibrary.ru

6.Оценка качества освоения программы

Итоговая аттестация проводится в виде экзамена.