областное государственное бюджетное
профессиональное образовательное учреждение
«Смоленская академия профессионального образования»

УТВЕРЖДАЮ
Директор ОГБПОУ СмолАПО
М. В. Белокопытов

ДОПОЛНИТЕЛЬНАЯ
ОБЩЕОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА
на базе мастерских для школьников
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
(14 часов)

автор-составитель:
Панина Наталья Владимировна
Преподаватель, СмолАПО

Смоленск 2020 год

ИНФОРМАЦИОННАЯ КАРТА

Цифровизация изменила мир. Изменения коснулись нашего стиля жизни, досуга, подхода к работе и обучению. Каждая организация, которая хочет предоставлять услуги заказчикам и сотрудникам, должна защищать свою сеть. Система сетевой безопасности также помогает защитить конфиденциальную информацию от атак. В конечном счете речь идет и о защите репутации.

Кибербезопасность, или информационная безопасность — новая перспективная сфера, в которой есть разные профессии.

Любая кибератака — это попытка получить несанкционированный доступ к компьютерной системе, инфраструктуре, сети или любому другому интеллектуальному устройству. Таким образом хакеры могут украсть базу клиентов компании, данные паспорта или банковской карты, похитить информацию, составляющую государственную тайну, нарушить систему жизнеобеспечения страны и даже вывести из строя систему противоракетной обороны.

Кибератаки стали одним из главных рисков, с которым сталкиваются люди и компании по всему миру. Это происходит из-за того, что вырос уровень разработки ПО: программы уже не пишут с нуля, а во многом собирают из готовых частей: библиотек и «фреймворков». При этом одной и той же библиотекой могут пользоваться сотни тысяч человек. Взломав такую библиотеку один раз, хакеры могут получить доступ сразу к сотням тысяч сайтов, которые ее используют. Это происходило и раньше, но сейчас популярность сторонних библиотек и количество новых программ, которые с их помощью создаются, стремительно растет. В 2019 году глобальный урон от киберпреступлений составил 2 трлн долларов.

Из-за этого сегодня спрос на специалистов по кибербезопасности превышает предложение. Уже через год мировой кибербезопасности понадобится 3,5 млн экспертов. Сравните: в 2014 требовался всего 1

млнчеловек! В Москве зарплата хороших специалистов начинается от 100 тыс. рублей и может доходить до 300-500 тыс. рублей в месяц. В то время как зарплата среднестатистического разработчика начинается от 45 тыс. рублей. Ожидается, что к 2027 году глобальные расходы на кибербезопасность достигнут 10 млрд долларов.

В России сейчас есть много программ в вузах, связанных с этой сферой, в самых разных городах.Защита от кибератак нужна любой компании или структуре, которая хранит информацию на цифровых носителях. В первую очередь это касается, конечно, финансовых структур, IT-компаний, органов государственной власти и оборонных ведомств.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Специалисты по кибербезопасности работают в крупных финансовых и IT-компаниях, ценность подобных кадров отмечается в государственных органах, оборонных ведомствах, где их основная задача – обеспечение национальной безопасности, предотвращение внедрения в государственную инфраструктуру

Целью дополнительной общеобразовательной программы профессиональных проб является формирование у учащихся 9-х классов интереса к профессии исодействие профессиональному самоопределению обучающихся посредством погружения в профессию.

Задачи программы:

- сообщение базовых сведений о профессии специалист по кибербезопасности;
- моделирование основных элементов профессиональной деятельности специалиста по кибербезопасности;
- выявление интересов обучающихся к данному виду практической деятельности;
- формирование у обучающихся реалистичных представлений о своих личностных характеристиках, способностях и об их соотношении с профессионально важными качествами представителя данной отрасли;
- определение уровня готовности обучающихся к выбору профессии.

Профессиональная проба рассматривается как средство актуализации профессионального самоопределения и активизации творческого потенциала личности школьников.

В рамках профессиональной пробы пройдут практико-ориентированные занятия на базе лабораторий вычислительной техники, где обучающиеся смогут попробовать себя в избранной профессии.

В процессе профессиональных проб обучающиеся приобретутначальные навыки профессиональной деятельности специалиста по кибербезопасности,

смогут приобрести навыки настройки параметров аутентификации Windows, управления доступом в Windows, освоить возможности режима защиты экрана, научиться управлять шаблонами безопасности.,соблюдая санитарно-гигиенические требованияправила безопасности труда.

Обучающиеся, освоившие программу профессиональных проб, должны ***знать и понимать:***

– знать основные понятия информационной безопасности;

- знать основные направления информационной безопасности.

Обучающиеся **должны *уметь***

- уметь настроить параметры аутентификации Windows,,

- уметь управлять шаблонами безопасности;

– уметь настроить параметры регистрации и аудита операционной системы;

При подведении итогов проходит обсуждение того, какими начальными профессиональными навыками овладели обучающиеся и какие сложности они испытывали при выполнении профессиональной пробы.

На этапе моделирования профессиональнойдеятельности в рамкахпрофессиональной пробы виды профессиональной деятельности преподавателя от начала деятельности до получения завершенного ее продукта (выполнение функциональных, должностных обязанностей, настройка элементов сети) разделяются на несколько циклов.

Каждый цикл содержит специфические особенности изучаемого вида профессиональной деятельности, демонстрирует стадии создания завершенного элемента продукта трудовой деятельности.

Выделенные циклы взаимосвязаны и в совокупности достаточно полно характеризуют содержание деятельности представителя изучаемой профессии, включая ситуации для проявления ПВК.

Циклы отличаются по целям и программно-инструментальным средствам, характеру, условиям и формам организации работы.

ТЕМАТИЧЕСКИЙ ПЛАН

№ п/п	Темы	Всего часов
1.	Основные понятия информационной безопасности	2
2.	Основные задачи и направления обеспечения информационной безопасности.	2
3.	Настройка параметров аутентификации Windows	2
4.	Многопользовательская работа	2
5.	Настройка параметров регистрации и аудита операционной системы	2
6.	Управление шаблонами безопасности	2
7	Итоговое тестирование	2
Итого		**14**

СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОЙ ПРОБЫ

Занятие № 1. Основные понятия информационной безопасности

Необходимо аргументированно обосновать, правильность или ошибочностькаждого из приведенных ответов (если ответ неверный, укажите, вчем заключается ошибка?) Используйте для поиска правильных ответов информационные ресурсы Internet.

1 .Что понимается под информационной безопасностью?

Ответ 1 Пол информационной безопасностью (ИБ) понимается состояние защищенности национальных интересов страны(жизненно-важных интересов личности, общества и государствана сбалансированной основе) в информационной сфере от внутренних и внешних угроз.

Ответ 2 В Доктрине информационной безопасности РФ защита от несанкционированного доступа к информационным ресурсам, обеспечение безопасности информационных и телекоммуникационных систем выделены в качестве важных составляющих национальных интересов РФ в информационной сфере.

Ответ 3 .Словосочетание «информационная безопасность» вразных контекстах может иметь различный смысл. В Доктринеинформационной безопасности РФ ИБ используется в широкомсмысле. Имеется в виду состояние защищенности национальныхинтересов в информационной сфере, определяемых совокупностьюсбалансированных интересов личности, общества и государства.

Ответ 4 В курсе «Информационная безопасность предпринимательской деятельности» термин ИБ используется в узком смысле. ПодИБ понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений.

2.Что такое информационная безопасность, каковы ее основные аспекты?

Ответ 1 .Информационная безопасность - это целостностьданных, доступность информации для всех авторизованныхпользователей и ее конфиденциальность.

Ответ 2 Информационная безопасность - многогранная область деятельности, в которой успех может принести толькокомплексный подход.

Ответ 3 Информационная безопасность - составная частьинформационных технологий.

Ответ 4 Информационная безопасность - защищенность потребностей объекта в качественной информации, необходимойему для нормального функционирования и развития.

3 В чем заключаются жизненно важные интересы в информационной сфере и угрозы жизненно важным интересам в информационной сфере?

Ответ 1 Зашита информации в смысле охраны персональных данных, государственной и служебной тайны и других видов ограниченного распространения.

Ответ 2 Компьютерная безопасность или безопасность данныхнабор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных в компьютерных сетях.

Ответ 3 защищенность информации и поддерживающей инфраструктуры от случайных и непреднамеренных воздействий естественного или искусственного характера.

Ответ 4 Под информационной и безопасностью понимают защищенность информации ОТ незаконного ознакомления, преобразованияи уничтожения, а также защищенность информационных ресурсов отвоздействий, направленных на нарушение их работоспособности.

Занятие № 2. Основные задачи и направления обеспечения информационной безопасности.

Необходимо аргументированно обосновать, правильность или ошибочностькаждого из приведенных ответов (если ответ неверный, укажите, вчем заключается ошибка?)

Используйте для поиска правильных ответов информационныересурсы Internet.

1 Каковы основные задачи в сфере обеспечения информационной безопасности?

Ответ 1 Развитие стандартизации информационных систем набазе общепризнанных международных стандартов и их внедрение длявсех видов информационных систем.

Ответ 2 Противодействие угрозе развязывания противоборства В информационной сфере.

Ответ 3 Организация международного сотрудничества пообеспечению информационной безопасности при интеграции России вмировое информационное пространство.

Ответ 4 Совершенствование и зашита отечественной информационной структуры, ускорение развития новых информационныхтехнологий и их широкое распространение с учетом вхождения России в глобальную информационную инфраструктуру.

2 Что такое политика безопасности?

Ответ 1.Политика безопасности строится на основе анализарисков, которые признаются реальными для информационной системы организации.

Ответ 2 Политика безопасности отвечает реальным рискаморганизации.

Ответ 3 Политика безопасности состоит из трех уровней.

Ответ 4 Первый уровень безопасности самый общий.

3 Каковы основные предметные направления защиты информации?

Ответ 1 Политика безопасности и гарантированности.

Ответ 2 Охрана государственной, коммерческой и др. тайн.

Ответ 3 Защита персональных данных.

Ответ 4 Защита интеллектуальной собственности.

Занятие № 3. Настройка параметров аутентификацииWindows

Практическая работа

1. Измените параметр «Пароль должен отвечать требованиям сложности» Политики паролей на «Включен» и после этого попробуйте изменить пароль своей учетной записи. Зафиксируйте все сообщения системы, проанализируйте и введите допустимый пароль. Этот пароль является результатом выполнения задания.

2. После успешного выполнения первого задания, измените пароль вашей учетной записи, а в качестве нового пароля укажите прежний пароль. Все сообщения зафиксируйте, проанализируйте и объясните поведение системы безопасности.

3. Проведите эксперименты с другими параметрами Политики учетных записей.

Занятие № 4. Многопользовательская работа

Практическая работа

1 Для Windows:
   a. создайте несколько учетных записей пользователя, в том числе одну – с возможностью администрирования;
   b. отключите гостевой доступ.
2 Установите пароль на заставку

Занятие № 5. Настройка параметров регистрации и аудита операционной системы

Практическая работа

1. Настройте параметры локальной политики безопасности ОС Windows.
2. Измените параметр «Пароль должен отвечать требованиям сложности» Политики паролей на «Включен» и после этого попробуйте изменить пароль своей учетной записи. Зафиксируйте все сообщения системы, проанализируйте и введите допустимый пароль. Этот пароль является результатом выполнения задания.
3. После успешного выполнения первого задания, измените пароль вашей учетной записи, а в качестве нового пароля укажите прежний пароль. Все сообщения зафиксируйте, проанализируйте и объясните поведение системы безопасности.
4. Проведите эксперименты с другими параметрами Политики учетных записей

Занятие № 6. Управление шаблонами безопасности

Практическая работа

1. Загрузите оснастку Шаблоны безопасности. Просмотрите значения имеющихся шаблонов в окне оснастки, например, шаблон безопасности compatws и его папки Политика учетных записей, Локальная политика и др.
2. Создайте на базе существующего Шаблона безопасности новый шаблон и дайте ему имя ПР-7.После этого зафиксируйте список шаблонов, скопировав изображение экрана в буфер и далее в файл для отчета.
3. Справка. По умолчанию шаблоны безопасности располагаются в каталоге

%SystemRoot%\Secunfy\Templates

.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

Реализация программы предполагает постепенное усложнение выполнения практических заданий профессиональной пробы в соответствииуровнем подготовленности обучающихся, внесение в содержание пробы элементов творчества и самостоятельности. При этом учитываются интересы, склонности, способности, профессионально важные качества личности, а также возрастные психолого-педагогические и валеологические особенности развития подростков.

Выполнение практических заданий в ходе профессиональной пробы осуществляется поэтапно. Каждый этап практического занятия предполагает выполнение обучающимися заданий, требующих овладения начальными профессиональными умениями и навыками, результатом чего является получение самостоятельно настроенной беспроводной сети.

Показатели качества выполнения практических заданий пробы:

- самостоятельность;
- соответствие конечного результата целям задания;
- обоснованность выбора программно-инструментальных средств;
- аккуратность;

активность и целеустремленность в достижении качественного результата;

- стремление выполнить условия и требования практического задания;
- проявление общих и специальных профессионально важных качеств(ПВК);
- рефлексия результатов собственной деятельности.
- В процессе реализации программы профессиональной пробы должное внимание уделяется обеспечению безопасности здоровья и жизни обучающихся.

МАТЕРИАЛЬНО – ТЕХНИЧЕСКОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОЙ ПРОБЫ

Для реализации программыпредусмотрена**Мастерская «Кибер-безопасности»** оснащена следующим оборудованием и программным обеспечением:

- Персональный компьютер в сборе: Processor - AMD Ryzen X8 R7-1700, DDR4 DIMM 32Гб, Видеокарта - ASUS GeForce GTX 1650 PHOENIX OC [PH-GTX1650-04G], SD накопитель A-DATA S11 Pro AGAMMIXS11P-512GT-C 512 Гб;
- Компьютерный монитор AOC 24" G2460VQ6;
- Клавиатура USB CBR KB 107;
- Компьютерная мышь USB CBR CM-302;
- Источник бесперебойного питания Powercom UPS RPT-800A EURO;
- Сервер [2U / 2 x Intel Xeon Silver 4210R (2.4GHz,10C) / 8 x 32Gb DDR4 2933, ECC R(24up) / 4x960Gb SSD SATA / 4 x 10GE / 2 x 800w;
- Управляемый Коммутатор Cisco WS-C2960L-48;
- Коммутатор L3 WS-C3650-24;
- Телевизор 50” LED Haier LE50K5500TF;
- Флипчат электронный SMART kapp 42;
- Интерактивная доска ScreenMedia;
- Проектор CASIO XJ-V110W с потолочным креплением и коммутацией;
- МФУ Canon i-SENSYS MF426dw;
- USB-токен JaCarta-2 PKI/ГОСТ (XL) JC-MediaKit-4 - "ПКJaCarta – MediaKit,
- РутокенЭЦП 2.0 64 кб;
- RDS-01 USB считывательключей Dallas Touch Memory (iButton);
- DS1996 сизогнутымбрелоком - электронныйключDallasTouchMemory (IButton);
- FindkeyHamster III (HFDU06S) - настольный биометрический считыватель;
- Установочный комплект. Средство защиты информации SecretNetStudio 8;

- Установочный комплект. Средство защиты информации vGate R2;
- Дистрибутив СКЗИ КриптоПро CSP версии 5.0 КС1 и КС2 на DVD;
- Формуляры DallasLock 8.0-К. Право на использование** (СЗИ НСД.СКН); Бессрочная лицензия DallasLock 8.0. Сертифицированный комплект для установки;
- Программное обеспечение клиентского доступа к виртуальным машинам AcademicVMwareWorkstation 15 ProforLinuxandWindows;
- СистемавиртуализацииVMWare ESXI 7.0, VMWare Workstation Pro, Oracle VirtualBox;
- ПО операционная система Windows 10 с интегрированной программной платформой .NET Framework, 4.8;
- ПО для просмотра документов в формате PDF AdobeReader DC;
- ПО для архивации 7-Zip;
- ПО офисный пакет MicrosoftOffice 2019;
- СистемавиртуализацииVMWare ESXI 7.0, VMWare Workstation Pro, Oracle VirtualBox;
- Антивирусное программное обеспечение KasperskyEndpointSecurity.

Литература

Дополнительные источники

1. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. -- М.: Книжный мир, 2009. -352 с.

2. Обеспечение информационной безопасности бизнеса Автор: Андриянов Виктор Издательство: Альпина Паблишерз Год: 2011 Страниц: 338 Формат: rtf, fb2 ISBN: 978-5-9614-1364-9 Размер: 11,72

3. А.Э. Саак, Е.В. Пахомов, В.Н. Тюшняков - Информационные технологии управления 2-е издание: Учебник для ВУЗов, 2-е издание – СПб.: Питер, 2009. – 320 с.: ил. – (Серия «Учебник для ВУЗов). ООО «Питер Пресс», 2009.

4. Корнеев И. К., Ксандопуло Г. Н., Машурцев В. А. – Информационный технологии: учеб. – М.: ТК Велби, Изд-во Проспект, 2009. – 224 с.

5. Федотова Е. Л. – Информационные технологии и системы: учеб.пособие. – М.: ИД «ФОРУМ»: ИНФРА-М, 2009. – 352 с.: ил. – (Профессиональное образование).

Электронные ресурсы:

1. http://wikisec.ru/ - энциклопедия по безопасности информации.