Образовательное частное учреждение
Дополнительного профессионального образования «Центр компьютерного обучения «Специалист» Учебно-научного центра при МГТУ им. Н.Э. Баумана»
(ОЧУ «Специалист»)

123242, город Москва, улица Зоологическая, дом 11, строение 2, помещение I, комната 11
ИНН 7701257303, ОГРН 1037739408189

Утверждаю:
Директор ОЧУ «Специалист»

_____ /Т.С.Григорьева/
«04» октября 2018 года

Дополнительная профессиональная программа повышения квалификации

«Защита веб-сайтов от взлома»

город Москва

Программа разработана в соответствии с приказом Министерства образования и науки Российской Федерации от 1 июля 2013 г. N 499 "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам".

Повышение квалификации слушателей, осуществляемое в соответствии с программой, проводится с использованием модульного принципа построения учебного плана с применением различных образовательных технологий, в том числе дистанционных образовательных технологий и электронного обучения в соответствии с законодательством об образовании.

Дополнительная профессиональная программа повышения квалификации, разработана образовательной организацией в соответствии с законодательством Российской Федерации, включает все модули, указанные в учебном плане.

Содержание оценочных и методических материалов определяется образовательной организацией самостоятельно с учетом положений законодательства об образовании Российской Федерации.

Структура дополнительной профессиональной программы соответствует требованиям Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам, утвержденного приказом Минобрнауки России от 1 июля 2013 г. N 499.

Объем дополнительной профессиональной программы вне зависимости от применяемых образовательных технологий, должен быть не менее 16 академических часов. Сроки ее освоения определяются образовательной организацией самостоятельно.

Формы обучения слушателей (очная, очно-заочная, заочная) определяются образовательной организацией самостоятельно.

К освоению дополнительных профессиональных программ допускаются:

- лица, имеющие среднее профессиональное и (или) высшее образование;
- лица, получающие среднее профессиональное и (или) высшее образование.

Для определения структуры дополнительной профессиональной программы и трудоемкости ее освоения может применяться система зачетных единиц. Количество зачетных единиц по дополнительной профессиональной программе устанавливается организацией.

Образовательная деятельность слушателей предусматривает следующие виды учебных занятий и учебных работ: лекции, практические и семинарские занятия, лабораторные работы, круглые столы, мастер-классы, мастерские, деловые игры, ролевые игры, тренинги, семинары по обмену опытом, выездные занятия, консультации, выполнение аттестационной, дипломной, проектной работы и другие виды учебных занятий и учебных работ, определенные учебным планом.

Аннотация. Этот курс посвящен методам защиты сайта и веб-сервера от взлома. Слушатель познакомится с архитектурой распространенных веб-серверов - IIS (Microsoft) и свободного веб-сервера Apache и узнают, как конфигурация сервера может повышать или понижать безопасность веб-сайтов. Рассмотрят разные виды атак на сайты и способы защиты от них. Подробно на курсе будут освещены такие виды взлома, как XSS-атаки и SQL-инъекции.

Полученные знания помогут слушателям оценить уровень защиты корпоративных ресурсов и провести мероприятия по ее укреплению. Особенно ценным окажутся для них комментарии и рекомендации преподавателей – опытных специалистов в сфере информационный безопасности, имеющих престижные сертификации EC-Council и Microsoft. Лабораторные работы позволят закрепить пройденный материал.

Цель программы: программа повышения квалификации направлена на совершенствование и (или) получение новой компетенции, необходимой для профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации.

Совершенствуемые компетенции

№	Компетенция	Направление подготовки
		ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО ОБРАЗОВАТЕЛЬНОГО СТАНДАРТА ВЫСШЕГО ОБРАЗОВАНИЯ ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ 09.03.02 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ (УРОВЕНЬ БАКАЛАВРИАТА)
		Код компетенции
1	способностью проводить выбор исходных данных для проектирования	ПК-4
2	способностью использовать математические методы обработки, анализа и синтеза результатов профессиональных исследований	ПК-25

Совершенствуемые компетенции в соответствии с трудовыми фикциями профессионального стандарта «Системный администратор информационно-коммуникационных систем" (Приказ Министерства труда и социальной защиты РФ от 5 октября 2015 г. N 684н "Об утверждении профессионального стандарта "Системный администратор информационно-коммуникационных систем").

№	Компетенция ОТФ	Направление подготовки
		ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ «Системный администратор информационно-коммуникационных систем»
		Трудовые функции (код)
1	B5 Администрирование прикладного программного Обеспечения инфокоммуникационной системы организации	B/01.5 Установка прикладного программного обеспечения B/02.5 Оценка критичности возникновения инцидентов при работе прикладного программного обеспечения. B/03.5 Оптимизация функционирования прикладного программного обеспечения B/04.5 Интеграция прикладного программного обеспечения в единую структуру инфокоммуникационной системы. B/05.5 Реализация регламентов обеспечения информационной безопасности прикладного программного обеспечения. B/06.5 Разработка нормативно-

		технической документации на процедуры управления прикладным программным обеспечением. B/07.5 Разработка требований к аппаратному обеспечению и поддерживающей инфраструктуре для эффективного функционирования прикладного программного обеспечения.

Планируемый результат обучения:

После окончания обучения Слушатель будет знать:

- Архитектуру, конфигурирование и создание сайтов IIS, Apache
- Типы атак на веб-сайты
- Принцип XSS-атак и SQL-инъекций

После окончания обучения Слушатель будет уметь:

- Создание сайтов на IIS
- Создание сайтов на Apache
- Сохраненные XSS
- Защита от XSS-атак
- Обход аутентификации с помощью SQL-инъекций
- Извлечение данных с помощью SQL-инъекций
- Изменение данных с помощью SQL-инъекций
- Защита от SQL-инъекций

Учебный план:

Категория слушателей:

- Системные администраторы безопасности, инженеры и аудиторы, работающие или предполагающие работать на средних и крупных предприятиях, вплоть до организаций корпоративного масштаба.
- Квалифицированные специалисты в области информационных технологий, включая администраторов предприятий, желающих улучшить свои знания и навыки в области безопасности веб-сайтов.
- Квалифицированные специалисты, которые хотят понять суть и методы защиты веб-сайтов.

Требования к предварительной подготовке:

M20410 Установка и конфигурирование Windows Server 2012 или эквивалентная подготовка.

Срок обучения: 16 академических часов, в том числе 8 аудиторных, 8 самостоятельно (СРС).

Форма обучения: очная, очно-заочная, заочная. По желанию слушателя форма обучения может быть изменена и/или дополнена.

Режим занятий: дневной, вечерний, группы выходного дня.

№ п/п	Наименование модулей по программе	Общая трудоемкость (акад. часов)	Всего ауд. ч	В том числе		СРС ,ч	Форма ПА[1]
				Лекций	Практ занятий		
1	Модуль 1. Архитектура, конфигурирование и создание сайтов IIS	4	2	2	0	*2*	
2	Модуль 2. Архитектура, конфигурирование и создание сайтов Apache	4	2	0	2	2	
3	Модуль 3. Типы атак на веб-сайты	2	1	0	1	1	
4	Модуль 4. Принцип XSS-атак	4	2	0	2	2	
5	Модуль 5. Принцип SQL-инъекций	2	1	0	1	1	Лаб. работа
		16	8	*2*	*6*	8	
	Итоговая аттестация	Лабораторная работа					

Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

Количество аудиторных занятий при очно-заочной форме обучения составляет 20-25% от общего количества часов.

Форма Промежуточной аттестации – см. в ЛНА «Положение о проведении промежуточной аттестации слушателей и осуществлении текущего контроля их успеваемости» п.3.3.

1. Календарный учебный график

Календарный учебный график формируется при осуществлении обучения в течение всего календарного года. По мере набора групп слушателей по программе составляется календарный график, учитывающий объемы лекций, практики, самоподготовки, выезды на объекты.

Неделя обучения	1	2	3	4	5	6	7	Итого часов
	пн	вт	ср	чт	пт	сб	вс	
1 неделя	4	0	4ИА	0	-	-	-	8
СРС	4	0	4	0	-	-	-	8
Итого:	8	0	8	0	-	-	-	16
Примечание: ИА – Итоговая аттестация (Лаб.раб.)								

2. Рабочие программы учебных предметов

[1] ПА – промежуточная аттестация.

Модуль 1. Архитектура, конфигурирование и создание сайтов IIS

- Архитектура IIS
- Основы безопасности веб сервера
- Создание сайтов на IIS
- Основы безопасности веб сайтов

Модуль 2. Архитектура, конфигурирование и создание сайтов Apache

- Архитектура Apache
- Создание сайтов на Apache

Модуль 3. Типы атак на веб-сайты

- Атаки на аутентификацию
- Атаки на авторизацию
- Атаки на клиентов
- Выполнение кода
- Раскрытие информации
- Логические атаки

Модуль 4. Принцип XSS-атак

- Отраженные XSS
- Сохраненные XSS
- Защита от XSS-атак

Модуль 5. Принцип SQL-инъекций

- Обход аутентификации с помощью SQL-инъекций
- Извлечение данных с помощью SQL-инъекций
- Изменение данных с помощью SQL-инъекций
- Защита от SQL-инъекций

4. Организационно-педагогические условия

Соблюдение требований к кадровым условиям реализации дополнительной профессиональной программы:

а) преподавательский состав образовательной организации, обеспечивающий образовательный процесс, обладает высшим образованием и стажем преподавания по изучаемой тематике не менее 1 года и (или) практической работы в областях знаний, предусмотренных модулями программы, не менее 3 (трех) лет;

б) образовательной организацией наряду с традиционными лекционно-семинарскими занятиями применяются современные эффективные методики преподавания с применением интерактивных форм обучения, аудиовизуальных средств, информационно-телекоммуникационных ресурсов и наглядных учебных пособий.

Соблюдение требований к материально-техническому и учебно-методическому обеспечению дополнительной профессиональной программы:

а) образовательная организация располагает необходимой материально-технической базой, включая современные аудитории, библиотеку, аудиовизуальные средства обучения, мультимедийную аппаратуру, оргтехнику, копировальные аппараты. Материальная база

соответствует санитарным и техническим нормам и правилам и обеспечивает проведение всех видов практической и дисциплинарной подготовки слушателей, предусмотренных учебным планом реализуемой дополнительной профессиональной программы.

б) в случае применения электронного обучения, дистанционных образовательных технологий каждый обучающийся в течение всего периода обучения обеспечивается индивидуальным неограниченным доступом к электронной информационно-образовательной среде, содержащей все электронные образовательные ресурсы, перечисленные в модулях дополнительной профессиональной программы.

5. Формы аттестации и оценочные материалы

Образовательная организация несет ответственность за качество подготовки слушателей и реализацию дополнительной профессиональной программы в полном объеме в соответствии с учебным планом.

Оценка качества освоения дополнительной профессиональной программы слушателей включает текущий контроль успеваемости и итоговую аттестацию.

Промежуточная аттестация по данному курсу проводится в форме выполнения практических работ, к итоговой аттестации допускаются слушатели, выполнившие все практические работы.

Результаты итоговой аттестации слушателей ДПП в соответствии с формой итоговой аттестации, установленной учебным планом, выставляются по двух бальной шкале («зачтено\незачтено»).

Слушателям, успешно освоившим дополнительную профессиональную программу и прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации.

Слушателям, не прошедшим итоговой аттестации или получившим на итоговой аттестации неудовлетворительные результаты, а также лицам, освоившим часть дополнительной профессиональной программы и (или) отчисленным из образовательной организации, выдается справка об обучении или о периоде обучения по образцу, самостоятельно устанавливаемому образовательной организацией. Результаты итоговой аттестации заносятся в соответствующие документы.

Итоговая аттестация проводится по форме представления учебных проектов и подготовки личного портфолио.

Текущая аттестация:

Практическая работа (выполнение заданий**):**

№п/п	***Тематика практического занятия***	***Форма ТА***
1	Создание сайтов на IIS	Лабораторная работа

Итоговая аттестация по курсу:

Лабораторная работа «Защита от SQL-инъекций».

Лабораторная работа - форма проведения аттестации (текущей, промежуточной, итоговой) с целью формирования профессиональных умений и навыков, совершенствования и (или) получения новой компетенции, необходимой для профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации.