28.04.21 04.08-12/25

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский государственный технический университет имени Н.Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

Институт современных образовательных технологий (ИСОТ)

УТВЕРЖДАЮ
Первый проректор-проректор
по учебной работе
_____Б.В. Падалкин
«28» 04 2021 г.

Дополнительное профессиональное образование

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА

ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Защита программ и данных

Регистрационный № 210408

Авторы программы:
д.ф.-м.н., доцент Басараб М.А.
Глинская Е.В.

Москва, 2021

СОГЛАСОВАНО:

Декан факультета Информатика и системы управления
МГТУ им. Н.Э. Баумана
д.т.н., профессор _____ А.В. Пролетарский
_____ (дата)

Начальник УМО ИСОТ
МГТУ им. Н.Э. Баумана _____ А.Н. Козлова
21.04.2021 (дата)

Оглавление

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДОПОЛНИТЕЛЬНОЙ ПРОФЕССИОНАЛЬНОЙ ПРОГРАММЫ

Дополнительная профессиональная программа (ДПП) «Защита программ и данных» подготовлена на основе:

– Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;

– требований Приказа Минобрнауки России от 01 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;

– методических рекомендаций-разъяснений Минобрнауки России по разработке дополнительных профессиональных программ на основе профессиональных стандартов от 22 апреля 2015 г. № ВК-1030/06;

– требований Приказа Министерства науки и высшего образования Российской Федерации от 19.10.2020 г. № 1316 «Об утверждении Порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности».

Реализация ДПП направлена на совершенствование имеющихся и/или получение новых компетенций, необходимых для профессиональной деятельности и повышения профессионального уровня в рамках имеющейся квалификации.

1.1. Цель ДПП

Целью ДПП является теоретическая и практическая подготовка программных реализаций, направленных на защиту программ и программных систем от анализа и вредоносных программных воздействий.

Сформировать у слушателей необходимые компетенции в области обеспечения защиты программ и данных.

1.2. Планируемые результаты обучения

Планируемые результаты обучения по ДПП:

– успешное освоение профессиональных компетенций в процессе изучения перечисленных в учебном плане тем;

– успешное освоение программы повышения квалификации;

– успешное прохождение итоговой аттестации и получение удостоверения о повышении квалификации по ДПП «Защита программ и данных».

1.3. Дополнительные характеристики ДПП

Перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения, определен приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. № 522н «Об утверждении профессионального стандарта «Специалист по защите информации в автоматизированных системах» (зарегистрировано в Минюсте России 28 сентября 2016 г., № 43857), регистрационный номер 843.

Наименование вида профессиональной деятельности: Обеспечение безопасности информации в автоматизированных системах (код 06.033).

Обобщенная трудовая функция: Разработка систем защиты информации автоматизированных систем.

Трудовая функция: Тестирование систем защиты информации автоматизированных систем (D/01.7).

1.4. Перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения. Характеристика компетенций, подлежащих совершенствованию, и/или перечень новых компетенций, формирующихся в результате освоения программы

Реализация ДПП направлена на совершенствование имеющихся и/или получение новых компетенций, необходимых для профессиональной деятельности и повышения профессионального уровня в рамках имеющейся квалификации.

Профессиональные компетенции (ПК) базируются на основании Приказа Министерства образования и науки Российской Федерации от 01 декабря 2016 г. № 1513 «Об утверждении федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.04.01 Информационная безопасность (уровень магистратуры)» (зарегистрировано 20 декабря 2016 г, регистрационный № 44823).

Перечень компетенций:

– способность анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты (ПК-1).

1.5. Соответствие видов деятельности и профессиональных компетенций и их составляющих

Трудовые функции			
Тестирование систем защиты информации автоматизированных систем (D/01.7)			
Профессио-нальные компетенции	**Практический опыт**	**Умения**	**Знания**
ПК-1	Проведение анализа структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности. Подбор инструментальных средств тестирования систем защиты информации автоматизированных систем.	Применять действующую нормативную базу в области обеспечения безопасности информации. Анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации.	Принципы построения и функционирования систем и сетей передачи информации. Особенности защиты информации в автоматизированных системах управления технологическими процессами. Технические средства контроля эффективности мер защиты информации.

2. УЧЕБНЫЙ ПЛАН ДПП

2.1. Категория слушателей ДПП

Для освоения ДПП допускаются лица, имеющие высшее образование уровня специалитет или магистратура в области информационной безопасности и/или освоившие дополнительное профессиональное образование в области информационной безопасности и имеющие практические навыки в данной области.

Программа так же будет интересна лицам, претендующим на должности: ведущий инженер-разработчик систем защиты информации, ведущий специалист по защите информации, руководитель проектов в области разработки систем защиты информации, руководитель отдела систем защиты информации, главный специалист по защите информации, руководитель отдела систем защиты информации, заместитель руководителя департамента (отдела) исследований и разработок, руководитель департамента (отдела) исследований и разработок.

2.2. Общая трудоёмкость программы, аудиторная и самостоятельная работа

Общая трудоемкость программы составляет 48 часов, из них 32 часа аудиторной работы и 16 часов самостоятельной работы.

2.3. Форма обучения

ДПП «Защита программ и данных» реализуется по очной форме обучения, возможна реализация программы с применением дистанционных образовательных технологий.

2.4. Учебный план

ДПП «Защита программ и данных» реализуется одним модулем.

№ п/п	Наименование тем	Всего, час	В том числе			Форма контроля
			Лекции	Практические занятия	Самостоятельная работа	
1.	Типовые уязвимости программного обеспечения и меры защиты от них	24	8	8	8	домашнее задание
2.	Жизненный цикл разработки безопасного программного обеспечения	24	8	8	8	домашнее задание
Итоговая аттестация		48	16	16	16	зачет

3. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

№ п/п	Наименование тем	1 день	2 день	3 день	4 день	5 день	6 день
1.	Типовые уязвимости программного обеспечения и меры защиты от них						
2.	Жизненный цикл разработки безопасного программного обеспечения						
Итоговая аттестация							

Минимальный срок освоения ДПП – 6 дней.

4. РАБОЧАЯ ПРОГРАММА ДПП

4.1. Рабочая программа модуля

4.1.1. Цель изучения модуля: теоретическая и практическая подготовка связанных с применением современных технологий анализа программных реализаций, защиты программ и программных систем от анализа и вредоносных программных воздействий.

4.1.2. Задачи изучения модуля:

- изучить средства и методы анализа программных реализаций;
- изучить средства и методы защиты программ от анализа;
- изучить модели функционирования и методы внедрения программных закладок;
- изучить средства и методы выявления программных закладок.

4.1.3. Планируемые результаты обучения

Процесс изучения учебной дисциплины направлен на формирование следующих ПК:

Код компетенции	Перечень планируемых результатов обучения по дисциплине	Формы и методы обучения, способствующие формированию и развитию компетенции
ПК-1	***Знать:*** – основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; – языки, системы, инструментальные программные и аппаратные средства, используемые для моделирования программного обеспечения и испытаний систем защиты. ***Уметь:*** – обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; – выполнять моделирование угроз безопасности информации и политик безопасности, реализованных защищенным программным обеспечением. ***Владеть:*** – методами и средствами выявления угроз безопасности автоматизированными системами; – комплексным рассмотрением вопросов моделирования угроз безопасности информации при разработке программного обеспечения.	Лекционные и практические занятия, самостоятельная работа с источниками информации и материалами аудиторных занятий

4.1.4. Содержание модуля

Тема 1. Типовые уязвимости программного обеспечения и меры защиты от них

Лекции (8 ч.). Безопасное (защищенное) программное обеспечение: основные понятия, термины и определения. Безопасность веб-приложений: SOP, cookie, идентификация, аутентификация, авторизация. Уязвимости веб-приложений: атаки типа XSS, SQLi, CSRF. Уязвимости веб-приложений: механизм CORS.

Практические занятия (8 ч.). Уязвимости веб-приложений: атаки типа XSS, SQLi, CSRF (практические аспекты). Уязвимости веб-приложений: механизм CORS (практические аспекты).

Самостоятельная работа (8 ч.).

Наименование темы	Дидактические единицы, вынесенные на самостоятельное изучение	Формы самостоятельной работы	Учебно-методическое обеспечение	Форма контроля
Безопасное (защищенное) программное	понятия, термины, определения, безопасность,	проработка материала лекций, практических	материалы аудиторных занятий,	домашнее задание

обеспечение. Безопасность, уязвимость веб-приложений	уязвимость, идентификация, аутентификация, авторизация	занятий и дополнительных источников информации	[1-3, 6]	

Примерные домашние задания:

1. Разработка алгоритма и программы выбора варианта антивирусной программы для защиты программного обеспечения компьютерной системы.

2. Разработка алгоритма и программы выбора варианта межсетевого экранирования для защиты программного обеспечения компьютерной системы.

3. Разработка алгоритма и программы выбора варианта системы обнаружения вторжений для защиты программного обеспечения компьютерной системы.

Тема 2. Жизненный цикл разработки безопасного программного обеспечения

Лекции (8 ч.). Жизненный цикл разработки безопасного программного обеспечения: основные понятия, термины и определения. Жизненный цикл разработки безопасного программного обеспечения по ГОСТ Р 56939. Моделирование угроз безопасности информации в жизненном цикле разработки безопасного программного обеспечения. Статический анализ кода в жизненном цикле разработки безопасного программного обеспечения. Тестирование проникновения в жизненном цикле разработки безопасного программного обеспечения.

Практические занятия (8 ч.). Моделирование угроз безопасности информации (практические аспекты). Применение статического анализа при разработке безопасного программного обеспечения. Тестирование проникновения при разработке безопасного программного обеспечения.

Самостоятельная работа (8 ч.).

Наименование темы	Дидактические единицы, вынесенные на самостоятельное изучение	Формы самостоятельной работы	Учебно-методическое обеспечение	Форма контроля
Жизненный цикл разработки безопасного программного обеспечения	понятия, термины, определения, анализ, программное обеспечение	проработка материала лекций, практических занятий и дополнительных источников информации	материалы аудиторных занятий, [2, 7, 8]	домашнее задание

Примерные домашние задания:

1. Разработка алгоритма и программы выбора варианта комплекса средств для защиты программного обеспечения автономного компьютера.

2. Разработка алгоритма и программы выбора варианта комплекса средств для защиты программного обеспечения локальной сети.

5. УСЛОВИЯ РЕАЛИЗАЦИИ ДПП

5.1. Организационные условия реализации ДПП

Наименование аудитории	Вид занятия	Наименование оборудования, программного обеспечения
Специализированная аудитория / компьютерный класс	Лекции, практические занятия	Персональные компьютеры, мультимедийный проектор, экран, доска, маркер, Microsoft Office, СПС КонсультантПлюс, Интернет, средства виртуализации, средства защиты информации, средства разработки, средства оценки эффективности защиты информации

5.2. Педагогические условия реализации ДПП

В реализации программы принимают участие ведущие преподаватели кафедры Информационная безопасность (ИУ-8) МГТУ им. Н.Э. Баумана, известные своими научными достижениями, как в теоретической, так и в практической области информационной безопасности автоматизированных систем.

5.3. Учебно-методическое обеспечение ДПП

1. Основы информационной безопасности: учеб. пособие для вузов / О.А. Акулов, Д.Н. Баданин, Е.И. Жук [и др.]. М.: Изд-во МГТУ им. Н.Э. Баумана, 2008. 159 с.

2. Бондарев В.В. Введение в информационную безопасность автоматизированных систем: учеб. пособие. М.: Изд-во МГТУ им. Н.Э. Баумана, 2016. 250 с.

3. Anderson R. Security Engineering. Wiley, 2008.

4. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. М.: Горячая линия – Телеком, 2000. 452 с.

5. Кевин Митник. Искусство обмана. М.: Компания АйТи, 2004. 416 с.

6. Брюс Шнайер. Секреты и ложь. Безопасность данных в цифровом мире. СПб.: Питер, 2003. 120 с.

7. Кулямин В. В. Методы верификации программного обеспечения. М.: Форум: ИНФРА-М, 2010. 97 с.

8. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации. М.: Радио и связь, 2012. 185 с.

5.4. Методические рекомендации

ДПП построена по тематическому принципу, каждая тема представляет собой логически завершенный раздел.

Преподавание программы основано на личностно-ориентированной технологии образования, сочетающей два равноправных аспекта этого процесса: обучение и учение. Личностно-ориентированный подход развивается при участии слушателей в активной работе на занятиях, направлен в первую очередь на развитие индивидуальных способностей, создание условий для развития творческой активности слушателя и разработку инновационных идей, а так же на развитие самостоятельности мышления, нахождение рационального варианта решения, сравнения и оценки нескольких подходов и т. п. Это способствует формированию приемов умственной деятельности по восприятию новой информации, ее запоминанию и осознанию, создания образов для сложных понятий и процессов, приобретению навыков поиска решений в условиях неопределенности.

Лекционные и практические занятия проводятся для приобретения навыков реализации знаний в предметной области. Занятия проводятся с использованием активных методов обучения.

Самостоятельная работа слушателей предназначена для внеаудиторной проработки материалов аудиторных занятий и источников информации не только рекомендованной, но из всех возможных источников, а также подготовки домашнего задания.

При изучении ДПП предусмотрены активные формы проведения занятий:

– управляемая дискуссия;

– разбор конкретных ситуаций.

6. ФОРМЫ ИТОГОВОЙ АТТЕСТАЦИИ ДПП

Итоговая аттестация проводится в форме зачета.

На зачете присутствуют преподаватели, принимающие участие в реализации программы.

По результатам итоговой аттестации слушателю выставляется оценка «Зачтено/Не зачтено»:

Оценка «Зачтено» выставляется слушателю, который:

- правильно ответил не менее чем на 75% вопросов зачета;
- продемонстрировал необходимые систематизированные знания и достаточную степень владения принципами предметной области программы, понимание их особенностей и взаимосвязь между ними в течение всего срока обучения по ДПП.

Оценка «Не зачтено» выставляется слушателю, который:

- ответил правильно менее чем на 75% вопросов зачета;
- имеет крайне слабые теоретические и практические знания, обнаруживает неспособность к построению самостоятельных заключений.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ИТОГОВОЙ АТТЕСТАЦИИ

7.1. Паспорт комплекта оценочных средств

Предметы оценивания	Объекты оценивания	Показатели оценки
ПК-1	***Знать:*** – основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; – языки, системы, инструментальные программные и аппаратные средства, используемые для моделирования программного обеспечения и испытаний систем защиты. ***Уметь:*** – обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; – выполнять моделирование угроз безопасности информации и политик безопасности, реализованных защищенным программным обеспечением. ***Владеть:*** – методами и средствами выявления угроз безопасности автоматизированными системами; комплексным рассмотрением вопросов моделирования угроз безопасности информации при разработке программного обеспечения.	– умение сравнивать; – умение анализировать; – умение классифицировать; – умение устанавливать причинно-следственные связи; – умение формулировать выводы

7.2. Комплект оценочных средств

Примерные варианты заданий к зачету:

Вариант 1

1. Безопасное (защищенное) программное обеспечение: основные понятия, термины и определения.

2. Тестирование проникновения в жизненном цикле разработки безопасного программного обеспечения.

3. Типовая архитектура, используемая в веб-технологиях, предусматривает наличие следующих взаимодействующий компонентов: веб-браузер – веб-сервер – сервер-приложений – система управления базами данных. В каком типе взаимодействия недостаток в механизме обработки входных данных может быть использована при выполнении атаки типа «SQL-инъекция»?

1) веб-браузер – веб-сервер;
2) веб-сервер – веб-браузер;
3) сервер приложений – система управления базами данных;
4) сетевое оборудование – сервер.

4. Какую угрозу может реализовать злоумышленник с использованием атаки типа «SQL-инъекция»?

1) получить несанкционированный доступ к информации;
2) перезаписать буфера для выполнения атаки типа «срыв стека»;
3) использовать память после ее освобождения;
4) все указанное выше.

5. Опишите основные контрмеры, которые могут использоваться для защиты от атаки типа CSRF.

Вариант 2

1. Безопасность веб-приложений: SOP, cookie, идентификация, аутентификация, авторизация.

2. Уязвимости веб-приложений: атаки типа XSS, SQLi, CSRF.

3. Какой ключевой недостаток лежит в основе атаки типа «SQL-инъекция»?

1) приложение доверяет данным без их проверки;
2) неспособность приложения отличить данные от кода;
3) обход механизма аутентификации;
4) обход принципа одинакового источника (same origin policy).

4. Примером какого типа защиты является экранирование символов (escaping)?

1) проверка входных данных (Validation);
2) черный список (Blacklisting);
3) белый список (Whitelisting);
4) приведение данных к доверенному формату (Sanitization).

5. Опишите сценарий атаки типа «Межсайтовая подделка скриптов» (cross-site request forgery, CSRF).

Вариант 3

1. Безопасное (защищенное) программное обеспечение: основные понятия, термины и определения.

2. Уязвимости веб-приложений: механизм CORS.

3. Предположим, что веб-приложение выполняет аутентификацию на основе данных, полученных из HTML-формы, с использованием SQL-запроса на основе подготовленного запроса

(prepared statements) языка программирования PHP. Что произойдет, если атакующий введет в поле HTML-формы следующую строку? FRANK' OR 1=1; --

1) введенный текст изменит структуру SQL-запроса, что может привести к обходу механизма аутентификации;
2) введенный текст будет воспринят в качестве пароля, аутентификация будет неуспешна;
3) приложение будет пытаться аутентифицировать пользователя, чье имя FRANK' OR 1=1;
4) введенный текст изменит структуру SQL-запроса, что приведет к синтаксической ошибке.

4. Почему использование только скрытых полей (hidden form fields) не является достаточным для реализации идентификации (отслеживания) сессии пользователя?

1) эти поля могут быть легко модифицированы пользователем;
2) эти поля не могут содержать бинарных данных;
3) идентификатор сессии пропадает при завершении работы браузера;
4) эти поля не могут включать информацию о времени действия идентификатора.

5. Опишите главное отличие атаки типа «отраженная XSS» («reflected XSS») от «сохраненный XSS» («stored XSS»).

Вариант 4

1. Использования средств автоматизированного тестирования при разработке типовых методик и тестов

2. Компоненты, обеспечивающие выполнение установленных политик информационной безопасности

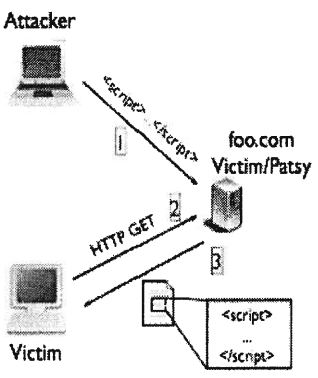
3. Что из перечисленного может быть вектором атаки, направленным на похищение или подделку сессионных куки-файлов (возможно более одного верного ответа)?

1) компрометация (поделка) браузера или сервера;
2) копирование значений куки-файла в момент ввода данных пользователем с клавиатуры;
3) чтение данных из незашифрованного потока данных;
4) предположение (угадывание) формата и структуры куки и восстановление данных.

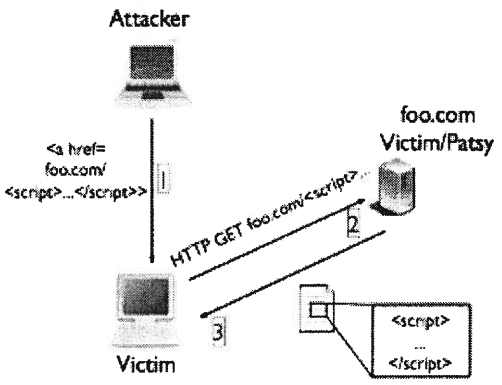
4. Для какого языка программирования наиболее характерен тег <script></script> в возвращаемой HTML-странице?

1) C;
2) Java;
3) PHP.

5. Javascript Рисунки, представленные далее, описывают два типа атаки типа «Межсайтовое выполнение запросов» (Cross-site scripting, XSS). Необходимо ответить на вопросы, представленные далее по тексту.



1



2

Какой тип атаки описывает каждый из рисунков?

1) рис.1 – сохраненный XSS, рис.2 – обратный XSS;
2) рис.1 – отраженный XSS, рис.2 –параллельный XSS;
3) рис.1 – сохраненный XSS, рис.2 – отраженный XSS;
4) рис.1 – отраженный XSS, рис.2 – сохраненный XSS.

Вариант 5

1. Опишите сценарий атаки типа «отраженный XSS» (с учетом схемы информационных потоков, представленных на рисунке).

2. Предположим, что браузер отсылает GET-запрос на адрес http://www.yan.com/accountinfo 20 февраля 2015 года. Какой куки (если он был сохранен) будет отослан вместе с этим запросом?

1) prefs=small:blue:refresh; expires=Sat, 1-Aug-2015; path=/specialoffers/; domain=.yan.com;
2) sessid=ABCDEFG; expires=Sat, 21-Feb-2015; path=/; domain=.yan.com;
3) lang=us-english; expires=Sat, 1-Aug-2015; path=/accountinfo/; domain=.fidelity.com;
4) edition=us; expires=Wed, 18-Feb-2015; path=/; domain=.yan.com.

3. Представлен следующий фрагмент исходного теста веб-приложения: *$query = "SELECT name FROM users WHERE uid = $UID"; // Then execute the query.*

(в данном случае поле $UID заполняется идентификатором пользователя UID, переданном в HTTP-запросе)

Необходимо ответить на следующие вопросы:

Объясните недостаток данного кода, актуальный для данного фрагмента.

Каким образом вы можете использовать данный недостаток для реализации атаки?

4. Опишите вектор атаки, направленный на удаление всех таблиц из БД

5. Опишите основные контрмеры, которые могут использоваться для защиты от подобного рода атак.

Вариант 6

1. Опишите сценарий атаки типа «сохраненный XSS» (с учетом схемы информационных потоков, представленных на рисунке).

2. Какой фактор чаще всего обеспечивает успешную реализацию компьютерных преступлений?

1) человеческий фактор;
2) уязвимости программного обеспечения;
3) нарушение логической структуры программных систем;
4) дефекты программного обеспечения.

3. Какой вид анализа не проводится на этапе компиляции программы?

1) лексический;
2) синтаксический;
3) семантический;
4) сигнатурный.

4. Какие требования по частоте проведения статического анализа прописаны в ГОСТ Р 56939?

1) нет необходимости проводить статический анализ ПО;
2) статический анализ необходимо проводить только на этапе разработки ПО;
3) статический анализ необходимо проводить на этапе разработки ПО и в качестве периодического контроля уже разработанного ПО;
4) статический анализ необходимо проводить только после разработки ПО в качестве периодического контроля.

5. Жизненный цикл разработки безопасного программного обеспечения: основные понятия, термины и определения.

Вариант 7

1. Опишите основные контрмеры, которые могут использоваться для защиты от атаки типа XSS

2 Какая из следующих классификаций представляет собой классификацию дефектов ПО?

1) CVE;
2) CWE;
3) NVD;
4) OSVDB.

3. Какой из перечисленных методов обычно не используется при проведении функционального тестирования?

1) метод черного ящика;
2) тестирование на основе классов эквивалентности;
3) позитивное тестирование;
4) тестирование на основе структур кода.

4. Какой из представленных видов тестирования направлен на проверку самой главной, важной функциональности разрабатываемого приложения?

1) смоук-тестирование;
2) расширенное тестирование;
3) тестирование доступности;
4) тестирование удобства использования.

5. Жизненный цикл разработки безопасного программного обеспечения по ГОСТ Р 56939.

Вариант 8

1. Моделирование угроз безопасности информации в жизненном цикле разработки безопасного программного обеспечения

2. Укажите процесс, который обычно не относится к управлению конфигурацией.

1) идентификация конфигурации;
2) управление изменениями;
3) отслеживание недостатков;
4) учет статуса конфигурации и аудит конфигурации.

3. Выберете наиболее полный набор документов, оформляемых обычно на практике в процессе осуществления функционального тестирования ПО.

1) описание тестовых процедур, отчет о результатах тестирования, отчет о недостатках;
2) описание тестовых процедур, план тестирования, отчет о результатах тестирования, отчет о недостатках, функциональная спецификация;
3) описание тестовых процедур, план тестирования, отчет о результатах тестирования, отчет о недостатках;
4) описание тестовых процедур, план тестирования, отчет о результатах тестирования, отчет о недостатках, запрос об изменении.

4. Укажите, что из перечисленного ниже следует относить к элементам конфигурации ПО.

1) исходные тексты;
2) проектная документация;
3) эксплуатационная документация;
4) все перечисленное.

5. Опишите главное отличие атаки типа XSS от атаки типа CSRF.

Авторы программы:

Заведующий кафедрой ИУ-8
МГТУ им. Н.Э. Баумана
д.ф.-м.н., доцент М.А. Басараб

Старший преподаватель кафедры ИУ-8
МГТУ им. Н.Э. Баумана Е.В. Глинская

8. ЛИСТ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ