МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ
Заведующий кафедрой
математического моделирования
М.Ш. Бурлуцкая
16.04.2024г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.13 Технологии разведки по открытым источникам данных (OSINT)

1. Код и наименование специальности:

10.05.04 Информационно-аналитические системы безопасности

2. Специализация:

Автоматизация информационно-аналитической деятельности

3. Квалификация выпускника:Специалист по защите информации

4. Форма обучения:Очная

5. Кафедра, отвечающая за реализацию дисциплины:

Кафедра математического моделирования

6. Составитель программы:Бурлуцкая М.Ш., д.ф.-м.н., доцент

7. Рекомендована:Научно-методическим советом математического факультета,протокол № 0500-03 от 28.03.2024

8. Учебный год:2028/2029 **Семестр:**9

9. Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

- изучение основ поиска, выбора и сбора разведывательной информации из общедоступных источников, а также её анализ.

Задачи учебной дисциплины:

- ознакомиться с анализом методологии и применяемых инструментов и сервисовдля OSINT в аналитической деятельности.

10. Место учебной дисциплины в структуре ОПОП:

Дисциплина «Технологии разведки по открытым источникам данных (OSINT)» относится к части, формируемой участниками образовательных отношений Блока 1. Дисциплины (модули).

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения:

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ПК-4	Способен осуществлять автоматизированную информационно-аналитическую поддержку процессов принятия решений	ПК-4.3	Способен искать и анализировать данные из открытых источников с целью обеспечения информационной безопасности	Знать: способы и методы анализа правоотношений, являющихся объектами профессиональной деятельности; Уметь: юридически правильно квалифицировать факты, события и обстоятельства; обосновывать решения, связанные с реализацией правовых норм в пределах должностных обязанностей; Владеть: навыками поиска и анализа данных из открытых источников с целью обеспечения информационной безопасности.

12. Объем дисциплины в зачетных единицах/час.— 4/144.

Форма промежуточной аттестации:зачет с оценкой.

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость		
		Всего	По семестрам	
			3 семестр	
Контактная работа		72	72	
в том числе:	лекции	36	36	
	практические	36	36	
	лабораторные	0	0	
	курсовая работа			
	контрольные работы			
Самостоятельная работа		72	72	
Промежуточная аттестация				
Итого:		**144**	**144**	

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК *
1. Лекции			
1.1	Общее представление об организации защиты данных в веб-ресурсах	Технологии получения и безопасной передачи информации в сети Интернет. Основные принципы организации защиты данных ввеб-ресурсах. Принципы безопасного использования веб-ресурсов. Понятиебезопасности приложений и классификация опасностей.Источники угрозинформационной безопасности и меры по их предотвращению.Регламенты иметоды разработки безопасных веб-приложений	
1.2	Современные угрозы безопасности веб-ресурсов	Классификация современных угроз безопасности веб-ресурсов OWASP Top 10.Уязвимости, связанные с внедрением команд и кода: SQL,NoSQL, OS, LDAP.Недостатки механизмов аутентификации. Уязвимости, ведущиек разглашениюконфиденциальной информации. Внедрение внешних XML-сущностей.Недостатки контроля доступа. Некорректная настройка параметров безопасности.Межсайтовое выполнение сценариев. Небезопаснаядесериализация.Использование компонентов с известными уязвимостями. Недостаткижурналирования и мониторинга	
1.3	Аудит безопасности и организация защиты данных в веб-ресурсах	Роль аудита безопасности веб-ресурсов при организации защиты данных в информационных системах. Тестирование напроникновение как важный элемент аудита безопасности веб-ресурса. Методы"черного", "серого" и "белого" ящика при тестировании на проникновение. Этапыпроведения тестирования на проникновение. DNS-разведка. Сбор информации изоткрытых источников (OSINT). Сбор информации о сервере. Сканированиеконтента. Фаззинг входных параметров. Поиск утечек данных. Тестированиеаутентификации. Отслеживание и перехват сессий. Атака с внедрением командОС. Включение файлов и обход каталогов. SQL-инъекции. XXE. Межсайтовоевыполнение сценариев. Межсайтовая подделка запроса. Атаки на логическиеуязвимости веб-ресурсов. Методы и средства организациизащиты данных в веб-ресурсах.	
1.4	Методы и средства безопасной разработки веб-ресурсов	Обзор рекомендаций OWASP по безопасной разработке веб-ресурсов. Безопасное взаимодействие и работа с данными из БД. Использованиебезопасных сторонних библиотек и фреймворков. Использование безопасныхалгоритмов аутентификации. Организация защиты от DDoS-атак. Шифрованиевеб-трафика с использованием SSL. Проверка корректности пользовательскихданных на клиенте и сервере. Безопасная конфигурацияинфраструктуры веб-ресурса.	
2. Практические занятия			
2.1	Общее представление об организации защиты данных в веб-ресурсах	Сбор данных о веб-ресурсе из открытых источников. Получение практических навыков поиска и анализаисходных данных веб-ресурса на основе открытых источников	
2.2	Современные угрозы безопасности веб-ресурсов	Выявление уязвимостей в веб-ресурсе методом активного сканирования. Получениепрактических навыков работы со сканерами безопасности, позволяющимивыявлять в веб-ресурсе известные уязвимости	

2.3	Аудит безопасности и организация защиты данных в веб-ресурсах	Организация защиты веб-ресурса от внедрения кода. Получение практических навыков проведения SQL- и других типов инъекций и организации защиты веб-ресурса от них	
2.4	Методы и средства безопасной разработки веб-ресурсов	Организация защиты веб-ресурса от атак XSS и XXE. Получение практических навыков проведения атаки XSS и XXE различных типов и организации защиты веб-ресурса от них	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (количество часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1	Общее представление об организации защиты данных в веб-ресурсах	8	8		16	32
2	Современные угрозы безопасности веб-ресурсов	10	10		20	40
3	Аудит безопасности и организация защиты данных в веб-ресурсах	10	10		20	40
4	Методы и средства безопасной разработки веб-ресурсов	8	8		16	32
	Итого:	**36**	**36**	**-**	**72**	**144**

14. Методические указания для обучающихся по освоению дисциплины:

Освоение дисциплины предполагает не только обязательное посещение обучающимся аудиторных занятий (лекций ипрактических занятий) и активную работу на них, но и самостоятельную учебную деятельность, на которую отводится 72 часа.

Самостоятельная учебная деятельность студентов по дисциплине «Технологии разведки по открытым источникам данных (OSINT)» предполагает выполнение следующих заданий:

1) самостоятельное изучение учебных материалов по разделам дисциплины с использованием основной и дополнительной литературы, информационно-справочных и поисковых систем;

2) подготовку к текущим аттестациям: выполнение практических заданий, поиск необходимых для работы материалов в Интернете.

Особое внимание обучающихся направляется на освоение необходимого в дальнейшим математического аппарата.

Вопросы лекционных и практических занятий обсуждаются на занятиях в виде устного опроса – индивидуального и фронтального. При подготовке к лекционным и практическим занятиям, обучающимся важно помнить, что их задача, отвечая на основные вопросы плана занятия и дополнительные вопросы преподавателя, показать свои знания и кругозор, умение логически построить ответ, владение математическим аппаратом и иные коммуникативные навыки, умение отстаивать свою профессиональную позицию. В ходе устного опроса выявляются детали, которые по каким-то причинам оказались недостаточно осмысленными студентами в ходе учебных занятий. Тем самым опрос выполняет важнейшие обучающую, развивающую и корректирующую функции, позволяет студентам учесть недоработки и избежать их при подготовке к промежуточным аттестациям.

Все выполняемые студентами самостоятельно задания (выполнение контрольных и самостоятельных работ) подлежат последующей проверке преподавателем. Результаты текущих аттестаций учитываются преподавателем при проведении промежуточной аттестации.

В случае необходимости перехода на дистанционный режим обученияиспользуется электронный курс «Технологии разведки по открытым источникам данных (OSINT)»на портале «Электронный университет ВГУ»:https://edu.vsu.ru.

Там жеразмещены необходимые для усвоения курса материалы.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
1.	Якунин А.Г. Учебно-методическое пособие по дисциплине «Основы WEB-технологий».- Барнаул, АлтГТУ, 2011. 173 с.
2.	Теплюк П.А. Методические указания к лабораторным работам по дисциплине «Информационная безопасность баз данных». - Барнаул, АлтГТУ, 2020. 20 с.
3.	Защита Web-приложений : учебное пособие : / А. В. Скрыпников, Д. В. Арапов, В. В. Денисенко, Т. Д. Герасимова ; науч. ред. И. А. Хаустов ; Воронежский государственный университет инженерных технологий. – Воронеж : Воронежский государственный университет инженерных технологий, 2020.

б) дополнительная литература:

№ п/п	Источник
4.	Додонов А.Г., Ландэ Д.В., Прищепа В.В., Путятин В.Г. Конкурентная разведка в компьютерных сетях 2013. 248 с.
5.	Брюхомицкий, Ю. А. Безопасность информационных технологий : учебное пособие : в 2 частях : [16+] / Ю. А. Брюхомицкий ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2020. – Ч. 1. – 171 с.
6.	

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет):

№ п/п	Ресурс
7.	Сайт математического факультета ВГУ. Раздел, на котором размещены методические издания:https://math.vsu.ru/wp/?page_id=937.
8.	ЭБС «Университетская библиотека онлайн».
9.	Электронный каталог ЗНБ ВГУ :http://www.lib.vsu.ru .
10.	Электронный университет ВГУ: https://edu.vsu.ru/course/view.php?id=19958.

16. Перечень учебно-методического обеспечения для самостоятельной работы:

№ п/п	Источник
1.	Open source intelligence tools and resources handbook 2018 Aleksandra Bielska
2.	
3.	Положение об организации самостоятельной работы обучающихся в Воронежском государственном университете.

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ, электронное обучение (ЭО), смешанное обучение):

Дисциплина может реализовываться с применением дистанционных образовательных технологий, например, на платформе «Электронный университет ВГУ»(https://edu.vsu.ru).

18. Материально-техническое обеспечение дисциплины:

Учебная аудитория для проведения занятий лекционного и семинарского типа, текущего контроля и промежуточной аттестации; специализированная мебель.

Для самостоятельной работы используется класс с компьютерной техникой, оснащенный необходимым программным обеспечением, электронными учебными пособиями и законодательно-правовой и нормативной поисковой системой, имеющий выход в глобальную сеть.

Перечень необходимого программного обеспечения:

Ubuntu (бесплатное и/или свободное ПО, лицензия: https://ubuntu.com/download/desktop),

VisualStudioCommunity (бесплатное и/или свободное ПО, лицензия https://visualstudio.microsoft.com/ru/vs/community/)

LibreOffice (GNU LesserGeneralPublicLicense (LGPL), бесплатное и/или свободное ПО, лицензия: https://ru.libreoffice.org/about-us/license/)

Foxit Reader, браузер Mozilla Firefox, Opera или Internet.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочныесредства
1	Общее представление об организации защиты данных в веб-ресурсах	ПК-4	ПК-4.3	Тест
2	Современные угрозы безопасности веб-ресурсов			Контрольная работа
3	Аудит безопасности и организация защиты данных в веб-ресурсах			Практическая работа
	Методы и средства безопасной разработки веб-ресурсов			Тест
Промежуточная аттестация Форма контроля –зачетс оценкой				Перечень вопросов к зачету

20. Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1. Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств: устных опросов, проверки домашних заданий, самостоятельных работ, контрольной работы.

Для оценивания текущего контроля успеваемости и оценивания самостоятельной работы используются следующие ***показатели:***

1) знание основных понятий и методов;
2) умение применять полученные знания и навыки для решения задач, проводить анализ полученных решений;
3) владение навыками хранения, поиска, сбора, систематизации, обработки и использования информации.

Шкала оценок:

Зачтено: Выполнение заданий соответствует перечисленным показателям, обучающийся дает ответы на дополнительные вопросы, может быть не совсем полные. Демонстрирует умение решать задачи, возможно с некоторыми ошибками.

Не зачтено:Ответы не соответствуют ни одному из перечисленных показателей. Обучающийся демонстрирует фрагментарные знания и умения или их отсутствие.

20.2. Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется в форме собеседования по билетам с помощью нижеприведенных оценочных средств (перечень вопросов к зачету).

В билет включаются теоретический вопрос и задача из примерного перечня задач для контрольной работы.

В случае посещения обучающимся всех аудиторных занятий (лекций и практических занятий) и активной работы на них, успешного выполнения элементов текущей аттестации (самостоятельные работы), оценка за промежуточнуюаттестацию может быть выставлена по результатам текущих аттестаций.

Перечень вопросов к дифференцированному зачету:

1. Технологии получения и безопасной передачиинформации в сети Интернет.
2. Основные принципы организации защиты данных в веб-ресурсах. Принципы безопасного использования веб-ресурсов.
3. безопасности приложений и классификация опасностей. Источники угроз информационной безопасности и меры по их предотвращению.
4. Регламенты и методы разработки безопасных веб-приложений
5. Классификация современных угроз безопасности веб-ресурсов OWASP Top 10.
6. Уязвимости, связанные с внедрением команд и кода: SQL, NoSQL, OS, LDAP.
7. Недостатки механизмов аутентификации.
8. Уязвимости, ведущие к разглашению конфиденциальной информации.
9. Внедрение внешних XML-сущностей. Недостатки контроля доступа. Некорректная настройка параметров безопасности. Межсайтовое выполнение сценариев.
10. Небезопасная десериализация. Использование компонентов с известными уязвимостями.
11. Недостатки журналирования и мониторинга
12. Роль аудита безопасности веб-ресурсов приорганизации защиты данных в информационных системах. Тестирование на проникновение как важный элемент аудита безопасности веб-ресурса.
13. Методы "черного", "серого" и "белого" ящика при тестировании на проникновение. Этапы проведения тестирования на проникновение.
14. DNS-разведка. Сбор информации из открытых источников (OSINT).
15. Сбор информации о сервере. Сканирование контента. Фаззинг входных параметров.

16. Поиск утечек данных.
17. Тестирование аутентификации. Отслеживание и перехват сессий
18. Атака с внедрением команд ОС. Включение файлов и обход каталогов.
19. SQL-инъекции. XXE. Межсайтовое выполнение сценариев. Межсайтовая подделка запроса.
20. Атаки на логические уязвимости веб-ресурсов. Методы и средства организации защиты данных в веб-ресурсах.
21. Обзор рекомендаций OWASP по безопасной разработке веб-ресурсов.
22. Безопасное взаимодействие и работа с данными из БД.
23. Использование безопасных сторонних библиотек и фреймворков
24. Использование безопасных алгоритмов аутентификации.
25. Организация защиты от DDoS-атак.
26. Шифрование веб-трафика с использованием SSL.
27. Проверка корректности пользовательских данных на клиенте и сервере. Безопасная конфигурация инфраструктуры веб-ресурса.

Для оценивания результатов обучения на зачете используются следующие **показатели:**

1) знание теоретических основ;
2) умение решать задачи;
3) умение работать с алгоритмами методов и информационными ресурсами;
4) успешное прохождение текущей аттестации.

Для оценивания результатовна дифференцированном зачете используется **шкала*:*** «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Соотношение показателей, критериев и шкалы оценивания результатов обучения показаны в следующей таблице:

Критерии оценивания	Шкала оценок
Ответ соответствует всем перечисленным выше показателям, обучающийся дает ответы на дополнительные вопросы. Демонстрирует знание учебного материала.	«Отлично»
Ответ соответствует двум или более из перечисленных показателей, обучающийся дает ответы на дополнительные вопросы, может быть не совсем полные. Демонстрирует знание учебного материала, возможно с некоторыми ошибками.	«Хорошо»
Ответ соответствует одному из перечисленных показателей, обучающийся не дает ответы на дополнительные вопросы. Демонстрирует знание учебного материала с некоторыми ошибками.	«Удовлетворительно»
Ответ не соответствует ни одному из перечисленных показателей. Обучающийся демонстрирует фрагментарные знания и умения или отсутствие их.	«Неудовлетворительно»

20.3 Фонд оценочных средств сформированности компетенций студентов, рекомендуемый для проведения диагностических работ

1. Цель – осуществление взлома системы для получения несанкционированного доступа к чужой информации – преследуют….

1. хакеры
2. кракеры *
3. "шутники"

2. Они взламывают систему с целью ее разрушения ….

1. "вандалы" *
2. "шутники"
3. "взломщики"

3. Наука о методах обеспечения конфиденциальности ….

1. криптология
2. криптография *
3. криптограмма

4. Если ВС способна противостоять активным атакам со стороны нарушителя, целью которого является навязывание ложного сообщения, то она обеспечивает …

1. целостность и достоверность информации *
2. управление доступом
3. полную подконтрольность и подотчетность

5. Потенциально возможное происшествие, которое может быть преднамеренным или непреднамеренным и может оказать нежелательное воздействие на систему …

1. угроза *
2. атака
3. взлом

6. Все многообразие средств ЗИ принято подразделять на следующие классы:

1. технические, программные, криптографические средства
2. технические, программные, организационные, криптографические средства *
3. административно-технические, аппаратно-программные, организационно-правовые средства

Критерии и шкалы оценивания заданий ФОС:

1) Задания закрытого типа (выбор одного варианта ответа, верно/неверно):

- 1 балл – указан верный ответ;
- 0 баллов – указан неверный ответ.

2) Задания закрытого типа (множественный выбор):

- 2 балла – указаны все верные ответы;
- 0 баллов — указан хотя бы один неверный ответ.

3) Задания закрытого типа (на соответствие):

- 2 балла – все соответствия определены верно;
- 0 баллов – хотя бы одно сопоставление определено неверно.

4) Задания открытого типа (короткий текст):

- 2 балла – указан верный ответ;
- 0 баллов – указан неверный ответ.

5) Задания открытого типа (число):

- 2 балла – указан верный ответ;
- 0 баллов – указан неверный ответ.

Задания раздела 20.3 рекомендуются к использованию при проведении диагностических работ с целью оценки остаточных результатов освоения данной дисциплины (знаний, умений, навыков).