Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский ядерный университет «МИФИ»

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

КАФЕДРА СТРАТЕГИЧЕСКИХ ИНФОРМАЦИОННЫХ ИССЛЕДОВАНИЙ

ОДОБРЕНО УМС ИИКС

Протокол № 8/1/2024

от 28.08.2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

МЕТОДЫ И СРЕДСТВА ВЫЯВЛЕНИЯ УЯЗВИМОСТЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Направление подготовки (специальность) [1] 10.04.01 Информационная безопасность

Семестр	**Трудоемкость, кред.**	**Общий объем курса, час.**	**Лекции, час.**	**Практич. занятия, час.**	**Лаборат. работы, час.**	**В форме практической подготовки/ В**	**СРС, час.**	**КСР, час.**	**Форма(ы) контроля, экз./зач./КР/КП**
3	3	108	8	24	0		40	0	Э
Итого	3	108	8	24	0	15	40	0	

АННОТАЦИЯ

Курс для получения требуемого уровня знаний, умений и навыков студентов в области применения современных методов и средств выявления уязвимостей в программном обеспечении и аппаратно-программных комплексах, характерных для значимых объектов критической информационной инфраструктуры (КИИ), с учетом требований регуляторных документов и особенностей эксплуатации таких систем.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью освоения дисциплины является формирование у магистрантов компетенций в области применения современных методов и средств выявления уязвимостей в программном обеспечении и аппаратно-программных комплексах, характерных для значимых объектов критической информационной инфраструктуры (КИИ), с учетом требований регуляторных документов и особенностей эксплуатации таких систем.

Основными задачами изучения дисциплины являются:

• Ознакомление студентов с нормативно-правовой базой и методическими рекомендациями ФСТЭК России в области выявления и устранения уязвимостей в информационных системах КИИ.

• Изучение специфики программного обеспечения АСУ ТП и SCADA-систем как ключевого объекта защиты в КИИ и связанных с ним классов уязвимостей.

• Освоение современных методов и средств выявления уязвимостей, включая статический и динамический анализ, с учетом ограничений, накладываемых на проведение работ в действующих системах КИИ.

• Формирование навыков планирования и проведения работ по оценке защищенности ПО, анализа результатов и составления отчетной документации в соответствии с отраслевыми стандартами.

• Приобретение опыта работы с системами управления уязвимостями (Vulnerability Management) и базами данных уязвимостей (CVE) для объектов КИИ.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Данная учебная дисциплина входит в базовую часть профессионального модуля ООП «Обеспечение безопасности значимых объектов критической информационной инфраструктуры» ОС НИЯУ МИФИ 10.04.01 «Информационная безопасность».

Требования к «входным» знаниям, умениям и готовностям студента, необходимым при освоении данной дисциплины:

знать технологии систем безопасности и подходы безопасности; основы разработки и обеспечения безопасности приложений; потенциальные угрозы безопасности информации разрабатываемых программых приложений;

уметь оценивать знания по безопасности разработчиков; выполнять проверку кода на соответствие рекомендациям по безопасности; обеспечивать защиту разрабатываемых приложений: обнаружение, управление, противодействие и восстановление;

владеть основами детального описания архитектуры аппаратных средств; навыками тесстирования на уязвимость; обеспечения защиты разрабатываемых приложений; проверки систем безопасности.

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел хорошей физико-математической подготовкой, знаниями, умениями и навыками смежных дисциплин «Теоретические основы информации безопасности объектов», «Организационно-правовое и техническое обеспечение информационной безопасности безопасности», «Аудит информационной безопасности компьютерных систем», «Основы аттестации объектов информатизации».

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**

Профессиональные компетенции в соответствии с задачами и объектами (областями знаний) профессиональной деятельности:

Задача профессиональной деятельности (ЗПД)	**Объект или область знания**	**Код и наименование профессиональной компетенции; Основание (профессиональный стандарт-ПС, анализ опыта)**	**Код и наименование индикатора достижения профессиональной компетенции**
научно-исследовательский			
Анализ фундаментальных и прикладных проблем ИБ в условиях становления современного информационного общества; выполнение научных исследований в области ИБ; подготовка по результатам научных исследований отчетов, статей, докладов на научных конференциях	Фундаментальные и прикладные проблемы информационной безопасности; методы и средства проектирования, моделирования и экспериментальной отработки систем, средств и технологий обеспечения информационной безопасности значимых объектов критической информационной инфраструктуры	ПК-3 [1] - Способен самостоятельно ставить конкретные задачи научных исследований в области ИБ или информационно-аналитических систем безопасности и решать их с использованием новейшего отечественного и зарубежного опыта *Основание:* Профессиональный стандарт: 06.030	З-ПК-3[1] - Знать: руководящие и методические документы уполномоченных федеральных органов исполнительной власти, устанавливающие требования к организации и проведению аттестации и сертификационных испытаний средств и систем защиты сссэ от нсд, зткс; основные средства и способы обеспечения информационной безопасности, принципы построения средств и систем защиты сссэ от нсд,

			зткс; национальные, межгосударственные и международные стандарты, устанавливающие требования по защите информации, анализу защищенности сетей электросвязи и оценки рисков нарушения их информационной безопасности. ; У-ПК-3[1] - Уметь: организовывать сбор, обработку, анализ и систематизацию научно-технической информации, отечественного и зарубежного опыта по проблемам информационной безопасности сетей электросвязи.; В-ПК-3[1] - Владеть: организацией подготовки научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований.

4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Разделы учебной дисциплины, их объем, сроки изучения и формы контроля:

№ п.п	Наименование раздела учебной дисциплины	Недели	Лекции/ Практ. (семинары)/ Лабораторные работы, час.	Обязат. текущий контроль (форма*, неделя)	Максимальный балл за раздел**	Аттестация раздела (форма*, неделя)	Индикаторы освоения компетенции
	3 Семестр						
1	Фундаментальные основы и методы выявления уязвимостей	1-8	4/12/0		25	КИ-8	З-ПК-3, У-ПК-3, В-ПК-3
2	Специализированные аспекты защиты программного	9-16	4/12/0		25	КИ-16	З-ПК-3, У-ПК-3, В-ПК-3

	обеспечения объектов КИИ						
	Итого за 3 Семестр		8/24/0		50		
	Контрольные мероприятия за 3 Семестр				50	Э	З-ПК-3, У-ПК-3, В-ПК-3

* – сокращенное наименование формы контроля

** – сумма максимальных баллов должна быть равна 100 за семестр, включая зачет и (или) экзамен

Сокращение наименований форм текущего контроля и аттестации разделов:

Обозначение	**Полное наименование**
КИ	Контроль по итогам
Э	Экзамен

КАЛЕНДАРНЫЙ ПЛАН

Недели	**Темы занятий / Содержание**	**Лек., час.**	**Пр./сем., час.**	**Лаб., час.**
	3 Семестр	8	24	0
1-8	**Фундаментальные основы и методы выявления уязвимостей**	4	12	0
1	**Тема 1: Введение в анализ защищенности ПО. Основные понятия и классификации.** Базовые понятия: уязвимость, эксплойт, CVE/CWE. Классификация уязвимостей по типу, критичности, механизму эксплуатации. Современные тренды в области уязвимостей ПО.. Знакомство с реестром уязвимостей ФСТЭК России и NVD. Поиск информации по заданному ПО.	Всего аудиторных часов		
		1	1	0
		Онлайн		
		0	0	0
2	**Тема 2: Классификации уязвимостей (CWE) и методы их выявления.** Краткое содержание: Выполнение комплексного задания по анализу уязвимостей в программном обеспечении объекта критической информационной инфраструктуры. Классификации уязвимостей (CWE) и методы их выявления. Составление модели угроз для условного объекта КИИ. Анализ CWE Top 25.	Всего аудиторных часов		
		1	1	0
		Онлайн		
		0	0	0
3	**Тема 3: Статический анализ (SAST). Принципы и инструменты.** Статический анализ (SAST). Принципы и инструменты. Проведение статического анализа исходного кода простого приложения с использованием открытых SAST-инструментов (например, SonarQube). Анализ отчета.	Всего аудиторных часов		
		1	1	0
		Онлайн		
		0	0	0
4	**Тема 4: Статический анализ (SAST).** 3.Статический анализ безопасности приложений (SAST). Принципы работы. Анализ исходного кода и бинарных файлов. Инструменты и их настройка. Анализ отчетов SAST-сканеров.	Всего аудиторных часов		
		1	1	0
		Онлайн		
		0	0	0

5	**Тема 5: Динамический анализ (DAST). Сканирование сетевых сервисов.** Динамический анализ (DAST). Сканирование сетевых сервисов. Сканирование уязвимостей тестового веб-приложения и сетевых сервисов с помощью OWASP ZAP и nmap. Верификация результатов.	Всего аудиторных часов		
		0	2	0
		Онлайн		
		0	0	0
6	**Тема 6:Динамический анализ (DAST). Сканирование сетевых сервисов. (продолжение)** Сканирование уязвимостей тестового веб-приложения и сетевых сервисов с помощью OWASP ZAP и nmap. Верификация результатов.	Всего аудиторных часов		
		0	2	0
		Онлайн		
		0	0	0
7	**Тема 7: Динамический анализ (DAST). Оценка критичности уязвимостей (CVSS).** Расчет баллов CVSS v3.1 для списка выявленных уязвимостей. Ранжирование и составление плана устранения.	Всего аудиторных часов		
		0	2	0
		Онлайн		
		0	0	0
8	**Тема 8: Комплексный анализ тестового приложения.** Краткое содержание: Проведение полного цикла анализа тестового приложения с использованием изученных методов и инструментов.	Всего аудиторных часов		
		0	2	0
		Онлайн		
		0	0	0
9-16	**Специализированные аспекты защиты программного обеспечения объектов КИИ**	4	12	0
9	**Тема 9: Реверс-инжиниринг программного обеспечения. Базовый анализ исполняемых файлов.** Краткое содержание: Методы дизассемблирования и декомпиляции. Анализ обфусцированного кода. Инструменты реверс-инжиниринга. Практическое знакомство с IDA Pro и Ghidra. Анализ простых исполняемых файлов.	Всего аудиторных часов		
		1	1	0
		Онлайн		
		0	0	0
10	**Тема 10: Анализ вредоносного ПО.** Краткое содержание: Базовые приемы анализа малвари. Использование Ghidra для анализа подозрительных образцов.	Всего аудиторных часов		
		1	1	0
		Онлайн		
		0	0	0
11	**Тема 11: Веб-безопасность и анализ веб-приложений. Статический анализ веб-приложений** Краткое содержание: OWASP Top 10. Методы обнаружения уязвимостей в веб-приложениях. Современные угрозы веб-безопасности. Использование SAST-инструментов для анализа PHP/Java кода веб-приложений.	Всего аудиторных часов		
		1	1	0
		Онлайн		
		0	0	0
12	**Тема 12: Динамический анализ веб-приложений** Краткое содержание: Практическая работа с OWASP ZAP и Burp Suite. Тестирование веб-приложений на наличие уязвимостей.	Всего аудиторных часов		
		1	1	0
		Онлайн		
		0	0	0
13	**Тема 13: Анализ безопасности ПО АСУ ТП. Фаззинг промышленных протоколов.** Краткое содержание: Особенности программного обеспечения для АСУ ТП. Уязвимости промышленных протоколов. Специфика анализа embedded systems. Настройка фаззеров для тестирования реализации протоколов Modbus TCP. Анализ результатов.	Всего аудиторных часов		
		0	2	0
		Онлайн		
		0	0	0
14	**Тема 14: Анализ встроенных систем и firmware**	Всего аудиторных часов		

	Краткое содержание: Методы извлечения и анализа firmware встроенных устройств. Использование специализированных инструментов.	0	2	0
		Онлайн		
		0	0	0
15	**Тема15: Верификация исправлений уязвимостей. Сравнительный анализ патчей безопасности** Краткое содержание: Использование bindiff для анализа изменений в бинарных файлах после установки обновлений безопасности.	Всего аудиторных часов		
		0	2	0
		Онлайн		
		0	0	0
16	**Тема 16: «Комплексный кейс: анализ ПО объекта КИИ»** Краткое содержание: Выполнение комплексного задания по анализу уязвимостей в программном обеспечении объекта критической информационной инфраструктуры.	Всего аудиторных часов		
		0	2	0
		Онлайн		
		0	0	0

Сокращенные наименования онлайн опций:

Обозначение	**Полное наименование**
ЭК	Электронный курс
ПМ	Полнотекстовый материал
ПЛ	Полнотекстовые лекции
ВМ	Видео-материалы
АМ	Аудио-материалы
Прз	Презентации
Т	Тесты
ЭСМ	Электронные справочные материалы
ИС	Интерактивный сайт

ТЕМЫ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Недели	**Темы занятий / Содержание**
	3 Семестр
1	**ПЗ1: Работа с базами данных уязвимостей»** Практическая работа с National Vulnerability Database (NVD). Поиск, анализ и классификация уязвимостей для заданного программного обеспечения.
2	**ПЗ2: Настройка и использование статических анализаторов** Краткое содержание: Практическая работа с статическими анализаторами кода. Анализ примеров кода на C/C++ на наличие уязвимостей.
3	**ПЗ3: «Продвинутый статический анализ»** Краткое содержание: Глубокий анализ сложных случаев уязвимостей. Работа с ложными срабатываниями. Настройка правил анализа.
4	**ПЗ4: «Инструменты отладки и анализа памяти»** Практическое занятие: «Инструменты отладки и анализа памяти» Краткое содержание: Практическая работа с отладчиками GDB, WinDbg. Использование Valgrind для обнаружения утечек памяти.
5	**ПЗ5: «Обнаружение ошибок выполнения»** Краткое содержание: Применение AddressSanitizer, MemorySanitizer. Анализ дампов памяти. Обнаружение ошибок управления памятью.
6	**ПЗ6: «Настройка и использование AFL»** Краткое содержание: Практическая работа с American Fuzzy Lop. Настройка фаззера для тестовых приложений. Анализ результатов.
7	**ПЗ7: «Фаззинг сетевых протоколов»**

	Краткое содержание: Использование Boofuzz для фаззинга сетевых сервисов. Создание собственных правил фаззинга.Введите здесь подробное описание пункта
8	**ПЗ8: «Комплексный анализ тестового приложения»** Краткое содержание: Проведение полного цикла анализа тестового приложения с использованием изученных методов и инструментов.
9	**ПЗ9: «Базовый анализ исполняемых файлов»** Краткое содержание: Практическое знакомство с IDA Pro и Ghidra. Анализ простых исполняемых файлов.
10	**ПЗ10: «Анализ вредоносного ПО»** Краткое содержание: Базовые приемы анализа малвари. Использование Ghidra для анализа подозрительных образцов.
11	**ПЗ11: «Статический анализ веб-приложений»** Краткое содержание: Использование SAST-инструментов для анализа PHP/Java кода веб-приложений.
12	**ПЗ12: «Динамический анализ веб-приложений»** Краткое содержание: Практическая работа с OWASP ZAP и Burp Suite. Тестирование веб-приложений на наличие уязвимостей.
13	**ПЗ13: «Фаззинг промышленных протоколов»** Краткое содержание: Настройка фаззеров для тестирования реализации протоколов Modbus TCP. Анализ результатов.
14	**ПЗ14: «Анализ встроенных систем и firmware»** Краткое содержание: Методы извлечения и анализа firmware встроенных устройств. Использование специализированных инструментов.
15	**ПЗ15: «Сравнительный анализ патчей безопасности»** Краткое содержание: Использование bindiff для анализа изменений в бинарных файлах после установки обновлений безопасности.
16	**ПЗ16: «Комплексный кейс: анализ ПО объекта КИИ»** Краткое содержание: Выполнение комплексного задания по анализу уязвимостей в программном обеспечении объекта критической информационной инфраструктуры.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

• Кейс-стади: Разбор реальных инцидентов и уязвимостей (на примере CVE), связанных с объектами КИИ.

• Практико-ориентированные занятия: Выполнение заданий на основе имитационных моделей и стендов (виртуальные машины с эмуляцией SCADA-систем, такие как GRFICS).

• Проблемные лекции: Обсуждение нормативных требований и методических сложностей при проведении работ на реальных объектах КИИ.

• Самостоятельная исследовательская работа: Анализ открытых источников на предмет информации об уязвимостях в заданном классе ПО для КИИ.

• Групповые дискуссии: Обсуждение стратегий приоритизации устранения уязвимостей и управления рисками.

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств по дисциплине обеспечивает проверку освоения планируемых результатов обучения (компетенций и их индикаторов) посредством мероприятий текущего, рубежного и промежуточного контроля по дисциплине.

Связь между формируемыми компетенциями и формами контроля их освоения представлена в следующей таблице:

Компетенция	**Индикаторы освоения**	**Аттестационное мероприятие (КП 1)**
ПК-3	З-ПК-3	Э, КИ-8, КИ-16
	У-ПК-3	Э, КИ-8, КИ-16
	В-ПК-3	Э, КИ-8, КИ-16

Шкалы оценки образовательных достижений

Шкала каждого контрольного мероприятия лежит в пределах от 0 до установленного максимального балла включительно. Итоговая аттестация по дисциплине оценивается по 100-балльной шкале и представляет собой сумму баллов, заработанных студентом при выполнении заданий в рамках текущего и промежуточного контроля.

Итоговая оценка выставляется в соответствии со следующей шкалой:

Сумма баллов	**Оценка по 4-х балльной шкале**	**Отметка о зачете**	**Оценка ECTS**
90-100	5 – *«отлично»*	«Зачтено»	A
85-89	4 – «*хорошо*»		B
75-84			C
70-74			D
65-69	3 – «*удовлетворительно*»		
60-64			E
Ниже 60	2 – «*неудовлетворительно*»	«Не зачтено»	F

Оценка «отлично» соответствует глубокому и прочному освоению материала программы обучающимся, который последовательно, четко и логически стройно излагает свои ответы, умеет тесно увязывать теорию с практикой, использует в ответах материалы монографической литературы.

Оценка «хорошо» соответствует твердым знаниям материала обучающимся, который грамотно и, по существу, излагает свои ответы, не допуская существенных неточностей.

Оценка «удовлетворительно» соответствует базовому уровню освоения материала обучающимся, при котором освоен основной материал, но не усвоены его детали, в ответах присутствуют неточности, недостаточно правильные формулировки, нарушения логической последовательности.

Отметка «зачтено» соответствует, как минимум, базовому уровню освоения материала программы, при котором обучающийся владеет необходимыми знаниями, умениями и навыками, умеет применять теоретические положения для решения типовых практических задач.

Оценку «неудовлетворительно» / отметку «не зачтено» получает обучающийся, который не знает значительной части материала программы, допускает в ответах существенные ошибки,

не выполнил все обязательные задания, предусмотренные программой. Как правило, такие обучающиеся не могут продолжить обучение без дополнительных занятий.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

https://online.mephi.ru/

http://library.mephi.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

9. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

Настоящие методические указания раскрывают рекомендуемый режим и характер учебной работы по изучению теоретических разделов курса, практическому применению изученного материала, по выполнению самостоятельной работы путем использования лекционного материала. Методические указания служат основой мотивации студента к самостоятельной работе и не подменяют рекомендуемую учебную литературу.

Данные указания определяют взаимосвязь курса с другими учебными дисциплинами образовательной программы – «Методы и средства выявления уязвимостей программного обеспечения», место курса в различных областях науки и техники. В том числе в области защиты программых приложений; в профессиональной деятельности выпускника; требования образовательного стандарта к уровню его подготовки; содержание дисциплины, сущность и краткая характеристика входящих в нее разделов, их взаимосвязь, особенности организации образовательного процесса по данной дисциплине специальности.

Особенности изучения разделов дисциплины

В процессе изучения данной дисциплины необходимо использовать действующие правовые акты в области защиты информации и разработки приложений, организационно-распорядительные, нормативные и информационные документы ФСТЭК России, других уполномоченных органов государственной власти, а также соответствующие учебно-методические пособия, иллюстративный материал (презентации).

На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся теоретической основой построения измерительных комплексов по анализу защищенности объектов информатизации и проведению инструментальных специальных исследований при аттестации объектов информатизации по требованиям безопасности информации. Часть лекций может излагаться проблемным методом с привлечением студентов для решения сформулированной преподавателем проблемы. С целью текущего контроля знаний в ходе лекций могут использоваться различные приёмы тестирования.

Проведение лабораторных работ - не предусмотренно.

На практических занятиях выносятся вопросы уровня навыков и умений. Задания выполняются студентами с использованием сети Интернет. На каждом рабочем месте должен быть развернут персональный компьютер (АРМ) с выходом в интернет. Результаты, полученные в ходе практических занятий, используются студентами в качестве исходных данных при отработке итоговых пакетов документов.

В качестве форм промежуточного контроля полученных знаний (раздел 1 и 2) используются: контрольная работа и тестирование. Для повышения результатов контроля студентами (по их желанию) могут быть выполнены и использованы письменные работы (рефераты).

В процессе итогового контроля также могут использоваться результаты, полученные студентами на практических занятиях.

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Настоящие методические указания раскрывают рекомендуемый режим и характер учебной работы по изучению теоретических разделов курса, практическому применению изученного материала, по выполнению самостоятельной работы путем использования лекционного материала. Методические указания служат основой мотивации студента к самостоятельной работе и не подменяют рекомендуемую учебную литературу.

Данные указания определяют взаимосвязь курса с другими учебными дисциплинами образовательной программы - Обеспечение безопасности информации ключевых систем информационной инфраструктуры, место курса в различных областях науки и техники. В том числе в области информационной безопасности; объекты и виды данной работы в профессиональной деятельности выпускника; требования образовательного стандарта к уровню его подготовки; содержание дисциплины, сущность и краткая характеристика входящих в нее разделов, их взаимосвязь, особенности организации образовательного процесса по данной дисциплине специальности.

КЛР8, КЛР15 - максим.балл-25, мин. балл – 9. Раздел считается аттестованным при получении оценки не ниже минимальной по каждой контрольной работе и выполнении всех лабораторных работ раздела.

При неаттестации хотя бы по одному из разделов, студент не допускается к зачёту.

Автор(ы):

Арустамян Сас Сергеевич