Развитие киберполигона Ampire

Иван Бугай,
Руководитель направления,
«Перспективный мониторинг»

О компании ПМ

ПМ сегодня

14 лет

на рынке услуг SOC и исследования защищённости

9 лет

корпоративный Центр ГосСОПКА класса «А»

1700

выполненных ИБ проектов

30

действующих киберполигонов Ampire

450

проведенных киберучений

3500

ИБ специалистов прошли обучение на Ampire

Регионы присутствия

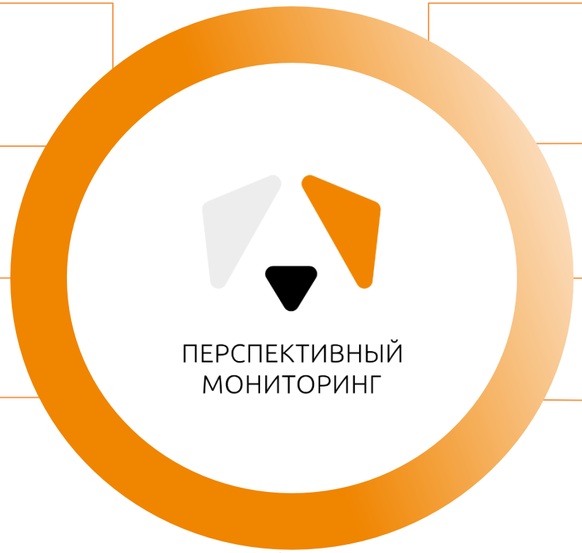
Направления деятельности

Исследование защищённости

- Пентест
- Аудит ИБ
- Оценка соответствия требованиям Банка России
- Категорирование объектов КИИ

SOC

- Коммерческий SOC
- Подключение к ГосСОПКА
- Расследование инцидентов ИБ
- Группа быстрого реагирования



Продукты

- Экспертные данные
- БРП AM Rules
- AM Threat Intelligence
- Киберполигон Ampire

Сквозная экспертиза по всем направлениям деятельности АО «ПМ»

Киберполигон Ampire

Учебно-тренировочная платформа для отработки навыков обнаружения, анализа и устранения последствий кибератак

- Практические занятия на «двойнике» реальной инфраструктуры
- Поддержка различных учебных форматов обучения – образовательный, тренировочный, соревновательный
- Полностью автоматические сценарии атак на основе реальных инцидентов и практики пентестеров и экспертов SOC ПМ
- Встроенные шаблоны инфраструктуры, СЗИ, сценарии атак, конфигуратор собственных сценариев
- Ежеквартальное обновление и наполнение платформы новыми узлами и сценариями
- ПАК, облачная и on-premises лицензии

50
комплексных сценариев «из коробки»

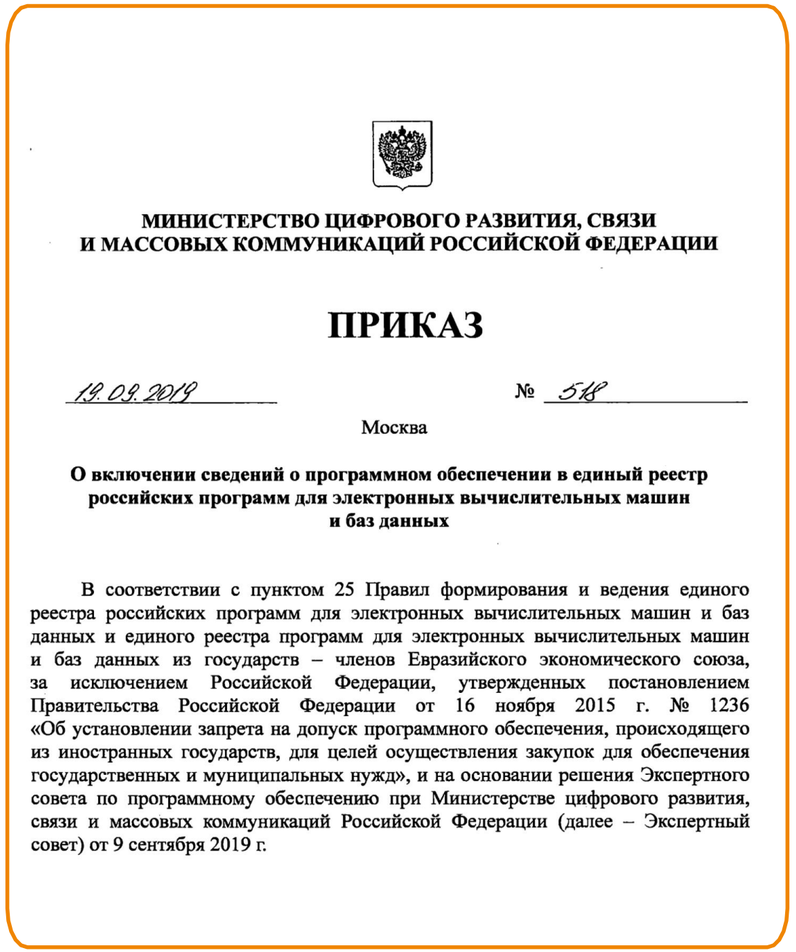
70
уязвимых узлов для конфигуратора сценариев

300
уязвимостей и последствий

Единый реестр российского ПО и регистрация в Роспатенте

AMPIRE

- **Единый реестр российских программ для электронных вычислительных машин и баз данных** от 20.09.2019 г. рег. номер ПО 5861
- **Класс ПО:** Информационные системы для решения специфических отраслевых задач
- **Решение уполномоченного органа:** Приказ Минкомсвязи России от 19.09.2019 №518
- **Свидетельство о государственной регистрации программы для ЭВМ** № 2019613098 выдано Роспатентом 07.03.2019 г.



МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

19.09.2019 № 518

Москва

О включении сведений о программном обеспечении в единый реестр российских программ для электронных вычислительных машин и баз данных

В соответствии с пунктом 25 Правил формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств – членов Евразийского экономического союза, за исключением Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд», и на основании решения Экспертного совета по программному обеспечению при Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации (далее – Экспертный совет) от 9 сентября 2019 г.

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2019613098

Программный комплекс обучения методам обнаружения, анализа и устранения последствий компьютерных атак «Ampire»

Правообладатель: *Закрытое акционерное общество «Перспективный мониторинг» (ЗАО «ПМ») (RU)*

Авторы: *Костюлин Илья Николаевич (RU), Наумова Александра Вячеславовна (RU), Овчинников Сергей Александрович (RU), Пушкин Александр Александрович (RU), Худой Юрий Игоревич (RU)*

Заявка № 2019612022
Дата поступления 01 марта 2019 г.
Дата государственной регистрации в Реестре программ для ЭВМ 07 марта 2019 г.

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев

Ampire удостоен премии Правительства РФ

За научно-практическую разработку
«Технология обучения мониторингу компьютерных атак и реагированию на компьютерные инциденты»

Форматы киберучений

Blue Team

Red Team

CSIRT

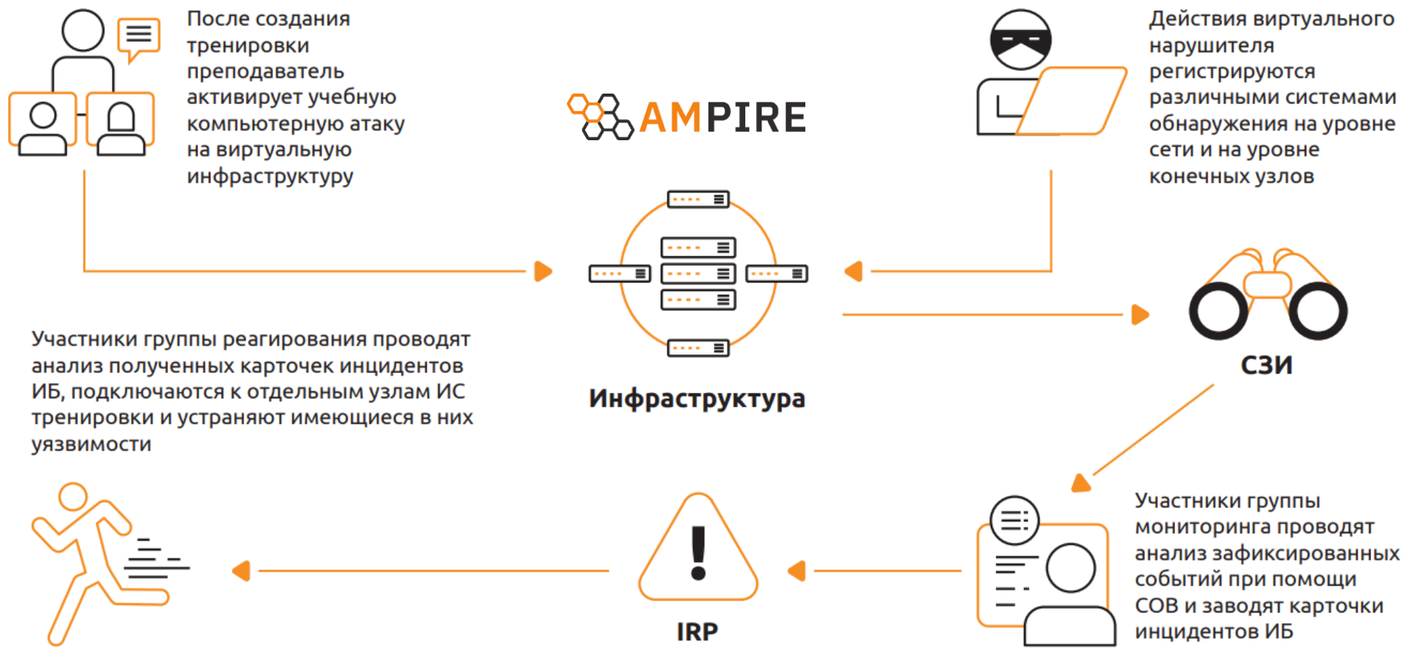
OSINT

- Blue Team – классический формат киберучений, где учатники отрабатывают навыки защиты от виртуального нарушителя
- Red Team – киберучения, направленные на понимание логики действий нарушителя. Задания для участников «красной» команды напоминают CTF и заключаются в успешном проникновении в инфраструктуру и эксплуатации уязвимости
- CSIRT (Computer Security Incident Response Team) – формат киберучений, в котором группы мониторинга и реагирования объединены в одну
- OSINT (Open Source Intelligence) – виртуальные лаборатории, предназначенные для повышения цифровой и ИБ грамотности. Основной формат Ampire Junior

Киберучения в формате Blue Team

AMPIRE

Схема проведения киберучений

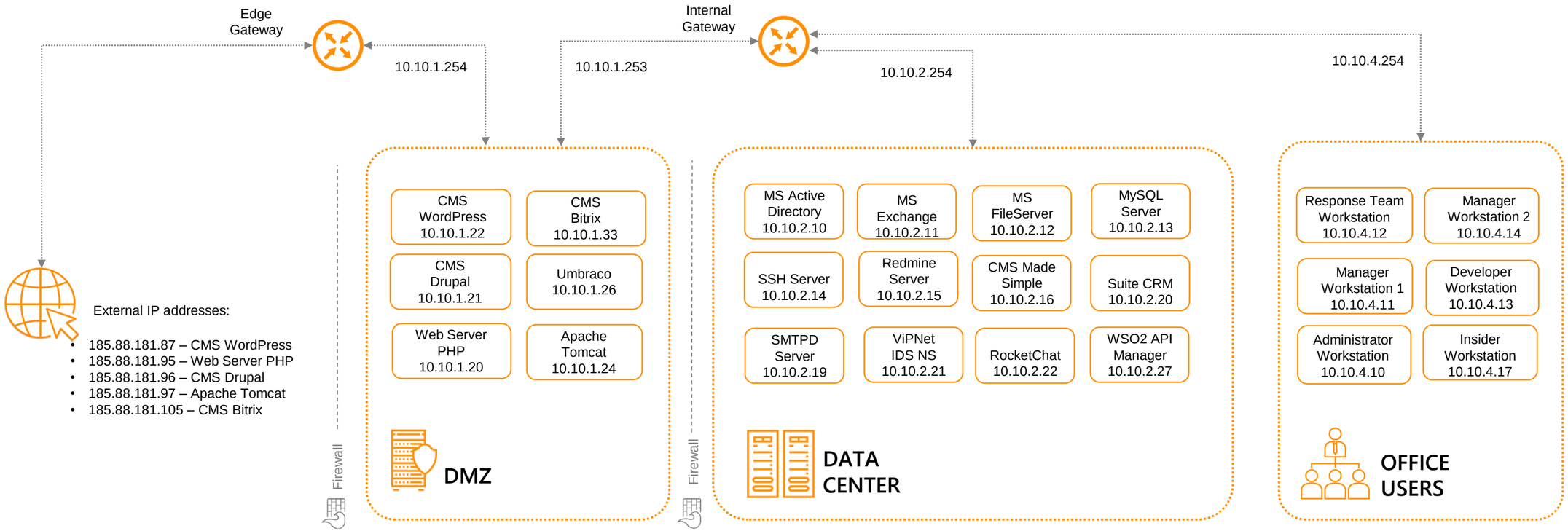


- анализ событий ИБ
- регистрация и расследование инцидентов ИБ
- устранение причин успешного выполнения КА
- командное взаимодействие

Задачи практических занятий

- Мониторинг и обнаружение компьютерных атак, направленных на элементы информационных систем организации;
- Работа с СПО для обнаружения и анализа событий ИБ;
- Разработка предложений по нейтрализации выявленных недостатков безопасности в ИС организации;
- Проведение расследований по локализации объектов атаки и внесение изменений в элементы ИС организации для нейтрализации выявленных угроз;
- Проведение мероприятий по оценке защищённости и соответствию требованиям ИС организации;
- Настройка и корректировка средств защиты информации для повышения уровня защищённости

Пример шаблона схемы сети

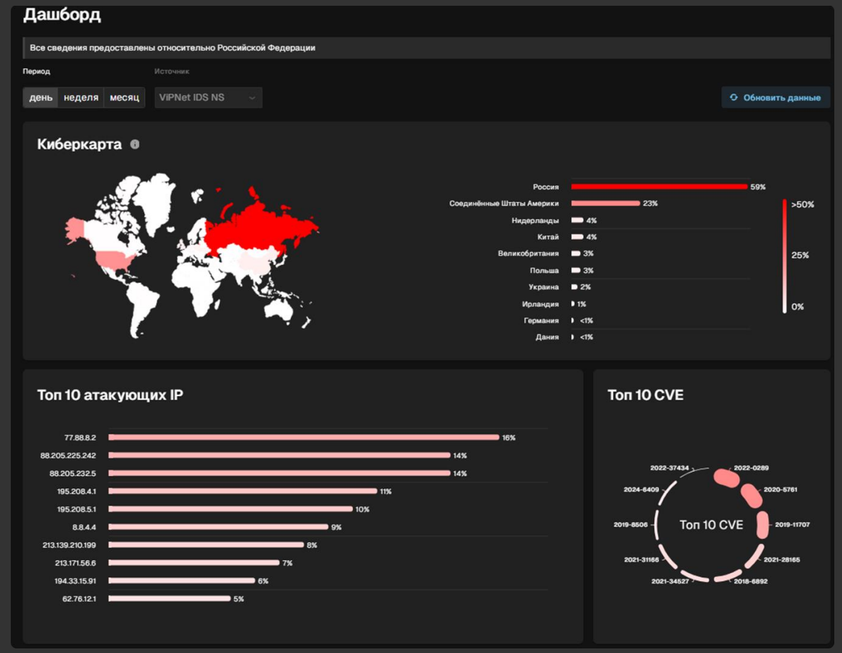


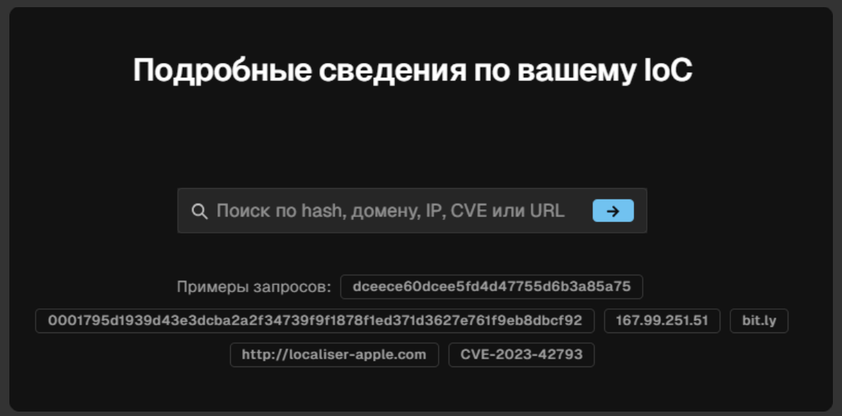
AM Threat Intelligence Portal

AMPIRE

/AMTIP

Интегрировали киберполигон Ampire с нашим TI-порталом





amtip.ru

Ampireметр

AMPIRE

30

действующих киберполигонов

450

проведенных киберучений

9

брендированных лабораторий

200

сертифицированных преподавателей

Пример применения – технический ВУЗ

- Занятия по Ampire на всех курсах
- 5-6 лабораторных работ в семестр на старших курсах
- До 4-5 занятий в день
- Использование Ampire в курсовых и дипломных проектах
- Использование Ampire в публичных мероприятиях и на олимпиадах
- Отдельная аудитория с сервером и рабочими местами под Ampire

Пример применения – регион

- Ampire размещен на мощностях ЦОД региона
- Доступ для организаций бюджетной сферы
- Регулярные киберучения
- Соответствие законодательству по киберучениям для предприятий КИИ
- Профильное обучение старшеклассников и молодых специалистов

Киберполигоны в вузах

AMPIRE

2017
Кемеровский государственный университет
Объединяем знания и людей

МТУСИ
Московский технический университет связи и информатики

МЭИ

МИРЭА
Российский технологический университет

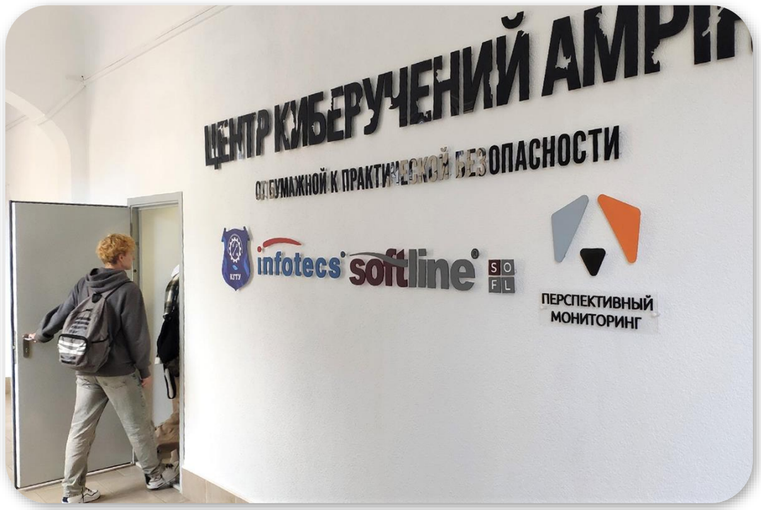
ТУСУР | TUSUR UNIVERSITY

ГУАП

НОВГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ ЯРОСЛАВА МУДРОГО

...

Центры киберучений Ampire



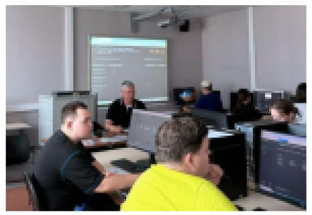
Поддерживаем Олимпиады и региональные соревнования

Перспективный мониторинг

🔒 **Всероссийская студенческая олимпиада по информационной безопасности**

Традиционно ПМ присутствует на финальном туре ВСО по ИБ. Сегодня студенты в рамках задания проходят сценарии на **киберполигоне Ampire**.

Перспективный мониторинг



🔵 **Всероссийская научная Летняя школа в СПбГУТ**

В этом году её участниками стали 60 студентов, которые представили 20 команд из вузов со всей страны.

Перспективный мониторинг

Смоленские школьники потренировались на Ampire Junior в формате OSINT на форуме «Свой код»

Перспективный мониторинг

🏆 Подведены итоги Ampire Trophy

🥇 Первое место заняла команда **Кемеровского государственного университета**

🥈 Второе место заняла команда **Санкт-Петербургского государственного университета аэрокосмического приборостроения**

🥉 Третье место заняла команда **Московского технического университета связи и информатики**

Поздравляем всех финалистов соревнований!

Карта киберучений Ampire
в 2024 году

AMPIRE

Киберполигон
Ampire Junior

Учебно-тренировочная платформа для занятий в области информационной безопасности для школьников

ИБ для школьников — это важно

На федеральном уровне

- Концепция информационной безопасности детей, утвержденная Председателем Правительства Михаилом Мишустиным в Распоряжении от 28 апреля 2023 года №1105-р
- Указ Президента РФ от 17 мая 2023 г. № 358
  «О Стратегии комплексной безопасности детей в Российской Федерации на период до 2030 года»
- Статья 5 ФЗ № 436
  «О защите детей от информации, причиняющей вред»
- ФЗ от 27.07.2006 № 149
  «Об информации, информационных технологиях и о защите информации»

ИБ для школьников — это важно

Запрос на повышение ИБ-грамотности на федеральном уровне

+

Спрос на специалистов ИБ на рынке

=

Необходимо повышать интерес к ИБ ещё до университетов

Что такое Ampire Junior?

В основе лабораторные работы (теория + практика)

Особенности	Виртуальная среда (шаблон) для практики	Занятия по темам ИБ (сценарии)	Методические материалы по темам	Теоретические и практические задания	Оценка выполнения заданий преподавателем
Навыки	Работа с информацией	Безопасное поведение в интернете	Базовая терминология в ИТ и ИБ	Оценка и фильтрация потока информации	Базовые принципы защиты информации

Реализованные сценарии

AMPIRE

Категории

Исследовательская активность

- Google Hacking
- Эффективный поиск в сети

Защита от информационного воздействия

- Доксинг
- Кибербуллинг
- Фейковые новости

Определить, является ли новость фейковой

- Фишинг
- Антифишинг
- Основы цифровой гигиены
- Основы криптографии

Открыть фишинговое письмо и увидеть заражение системы

Защита персональных данных

Расшифровать текст и зашифровать сообщение

Применение
в учебном процессе

Практические уроки по цифровой грамотности в рамках школьной программы

Школьники на практике изучают основы безопасной работы с компьютерами и мобильными устройствами, учатся определять вредоносные действия и защищать себя от негативного воздействия, защищать свои персональные данные, осваивают базовые навыки работы с программным и аппаратным обеспечением

Физическое и психологическое благополучие

Занятия на Ampire Junior предполагают практическое освоение материала, одновременно контролируя естественное стремление детей на практике узнать ответ на вопрос «А что будет, если...?». Благодаря увеличению осведомленности и возможности научиться в безопасной виртуальной среде правильно взаимодействовать с цифровым миром повышается общий уровень физической и психологической безопасности детей

Курсы дополнительного образования для школьников

Ampire Junior дополнительно используется для углубленного изучения и решения ИТ и ИБ задач в рамках факультативов, практикумов, дополнительных образовательных курсов, а также для занятий учеников в профильных ИТ классах. При этом занятия могут проводиться как в очном, так и в удаленном формате подключения

Соревнования и олимпиады

Проведение школьных, городских, районных и областных соревнований по информационным технологиям и информационной безопасности в различных форматах, включая конкурсы, CTF, олимпиады. Платформа позволяет проводить как индивидуальные, так и групповые соревновательные активности

Разработка собственных учебных заданий

Возможности платформы намного шире поставляемого набора лабораторных работ. Каждый учитель может интегрировать Ampire Junior в свою учебную программу, создавая дополнительные задания на основе заложенной базовой функциональности

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

AMPIRE

Спасибо
за внимание!

Иван Бугай

Руководитель направления по работе с ключевыми заказчиками
«Перспективный мониторинг»

+7 (916) 776-96-51

Ivan.Bugay@amonitoring.ru

t.me/pm_public amonitoring.ru ampire.team