Обучение студентов-программистов киберимунной разработке ПО

при поддержке Лаборатории Касперского

KasperskyOS

2023, Октябрь

ИБ-грамотность в фокусе ИТ вузов

- Рост угроз информационной безопасности и импортозамещение стали драйверами роста образовательных программ по защите информации

приоритет2030^
лидерами становятся

ИМПОРТОЗАМЕЩЕНИЕ

ВФФС
ВСЕРОССИЙСКАЯ ФЕДЕРАЦИЯ ФИДЖИТАЛ СПОРТА

Федерация спортивного программирования

Дефицит специалистов по информационной безопасности в России от 50 000 до 100 000 человек

- Ведущие ИТ ВУЗы уже осваивают кибериммунную методологию разработки программных продуктов АО «Лаборатория Касперского»

ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УНИВЕРСИТЕТ СИНЕРГИЯ

Санкт-Петербургский государственный университет
1724

МИРЭА
Российский технологический университет

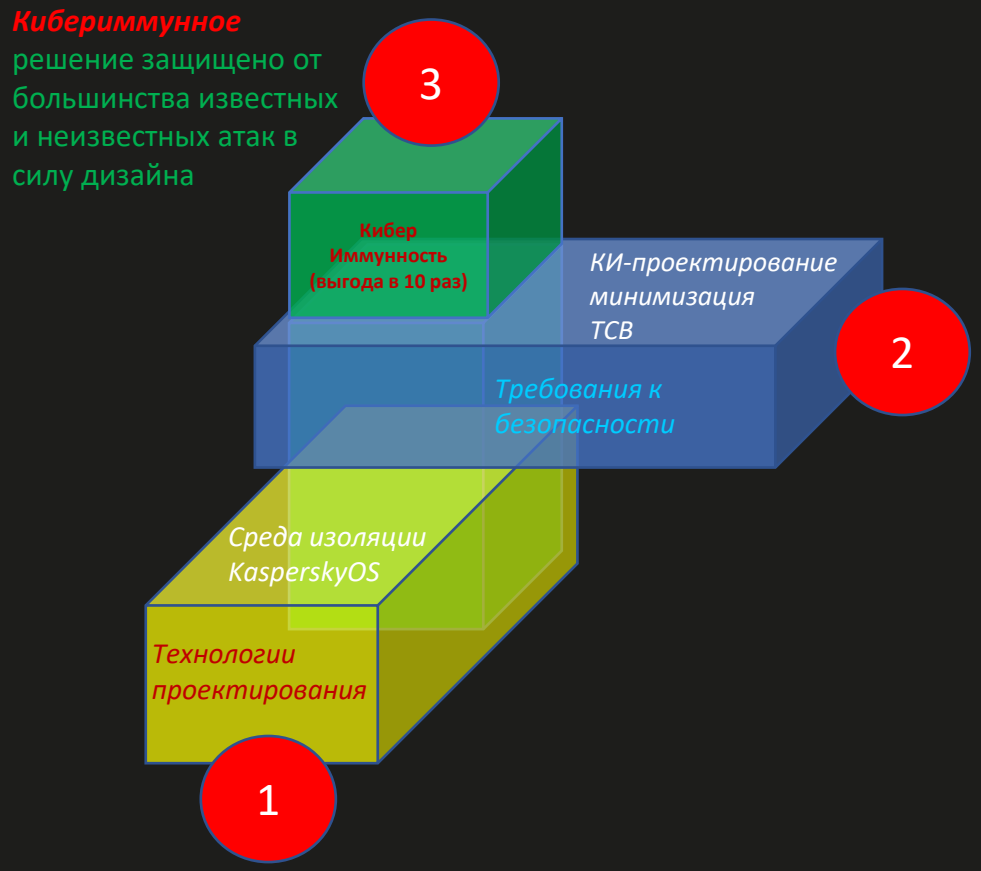
МАИ

Петрозаводский государственный университет
ПетрГУ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ
Cum nobis in futuro
МГОТУ

ВЫСШАЯ ШКОЛА ЭКОНОМИКИ

Кибериммунитет – это просто!



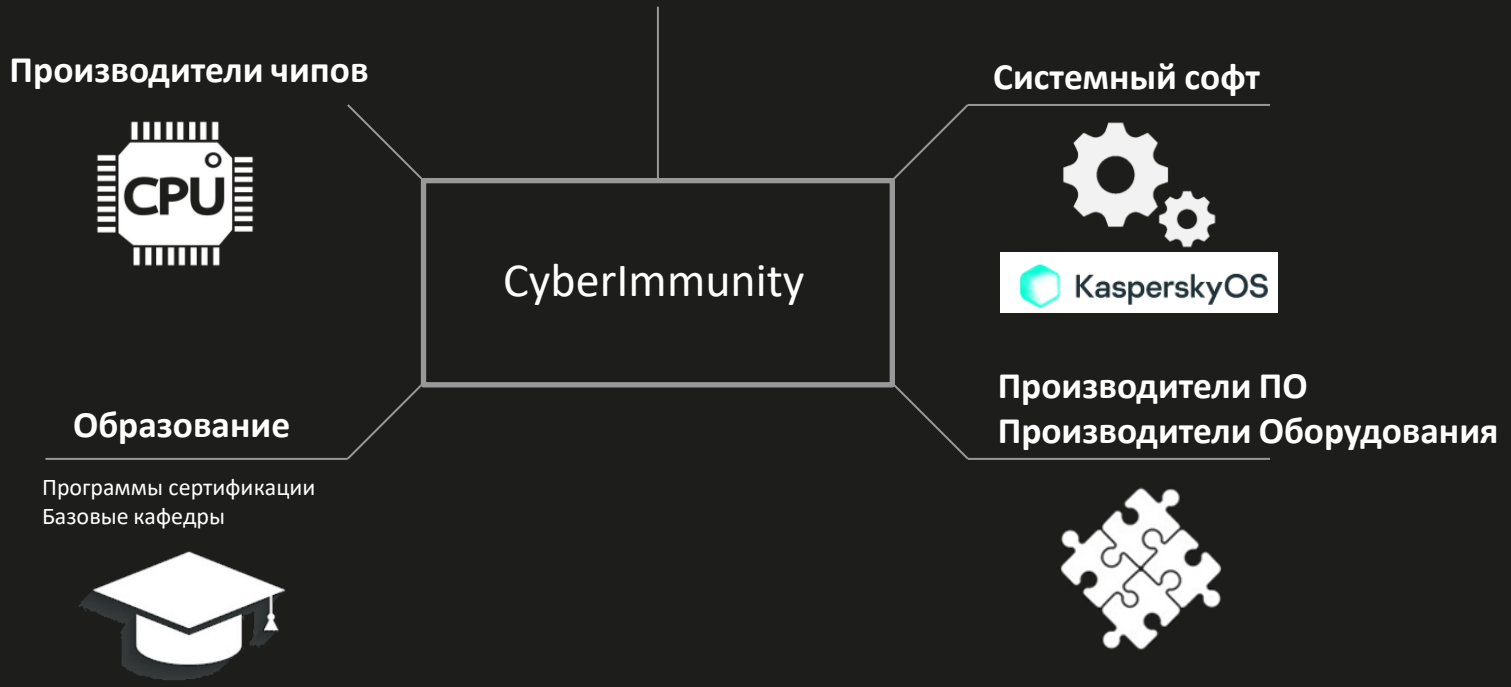
Кибериммунитет – сочетание лучших практик политик безопасной изоляции компонентов ПО и минимизации их доверенной базы, что дает качественный рост защищенности от известных и неизвестных атак в силу дизайна системы

Кибериммунитет реализует подход Secure by Design (aka конструктивная информационная безопасность) создавая ПО/ПАК без влияния уязвимостей отдельных его частей на доверие к решению в целом

Кибериммунитет основан на архитектурных принципах систем с разделение доменов – ПНСТ РФ 818-2023, 819-2023 разработанных на базе ТК по стандартизации 194 «Кибер-физические системы».

Кибериммунитет – точка объединения индустрии конструктивно безопасных решений

CyberImmunity это сочетание методологии и технологий, объединяющая индустрию по созданию конструктивно безопасных решений



Кибериммунитет – международная история

industrial internet CONSORTIUM

- “MILS Architectural Approach Supporting Trustworthiness of the IIoT Solutions”, 2021

Architectural approach behind KasperskyOS as a strategy for creating IT systems

Source

ARC Advisory Group

- “From Cybersecurity to Cyber Immunity in IIoT”, 2021

An expert view on Kaspersky's Cyber Immunity concept: Kaspersky Cyber Immunity – a new approach to digital transformation

Source

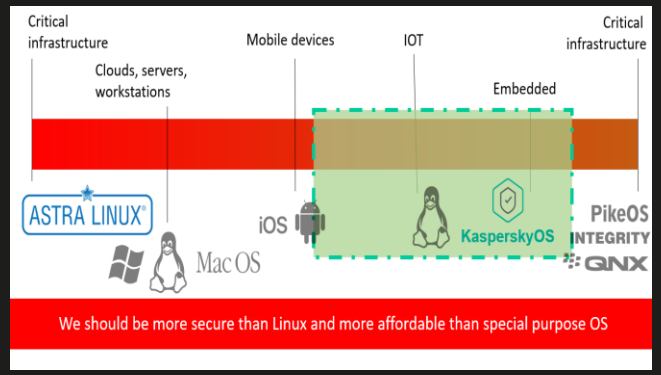
Gartner

- “Vendor to watch” for its KasperskyOS

Market Trends: Software-Defined Vehicles Will Disrupt the Automotive Supply Chain

Source

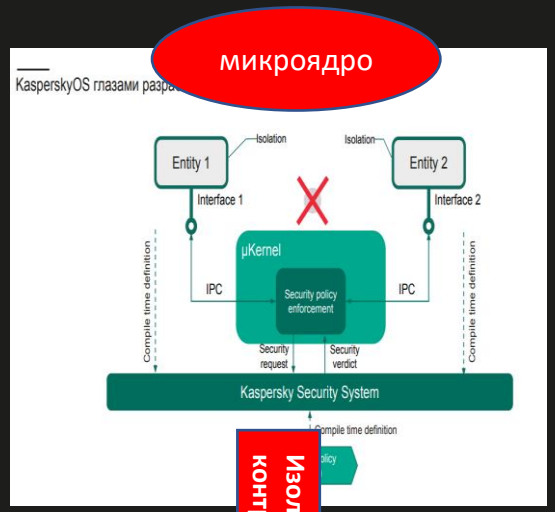
1 Микро-ядерная KasperskyOS с фокусом на безопасность



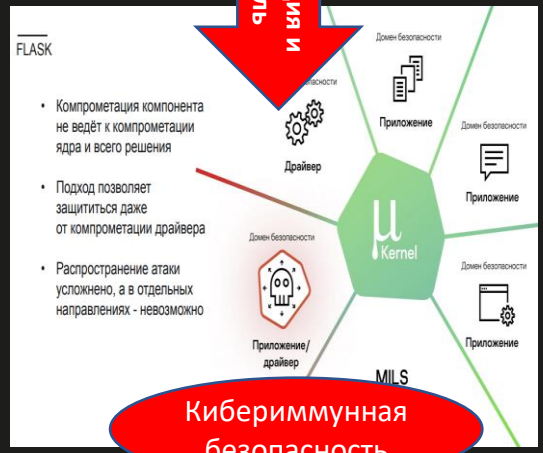
Отечественная микроядерная KasperskyOS дает гораздо больше конструктивной безопасности своим решениям, чем *nix ОС общего назначения
при затратах существенно ниже
чем при использовании специализированных ОС

Особенности KasperskyOS

- KasperskyOS это не Linux, но 100% отечественная ОС на микроядре в 1000 раз меньшего и доверенного, чем монолитные ОС как Linux
- Безопасность в KasperskyOS отличается от сложного программирования DAC/MAC в seLinux на уровне Linux Security Modules (LSM), упрощенным администрированием IPC политик взаимодействия изолированных компонент KasperskyOS с реализацией RBAC и качественным ростом уровня защиты
- Открытое SDK публичной версии KasperskyOS для создания собственных решений
- Поддержка KasperskyOS на всех современных (включая отечественные) процессорных платформах, имеет высокую производительность, растущее сообщество разработчиков



Изоляция и контроль



Кибериммунность реализует secure by design MILS-изоляцию компонент решения

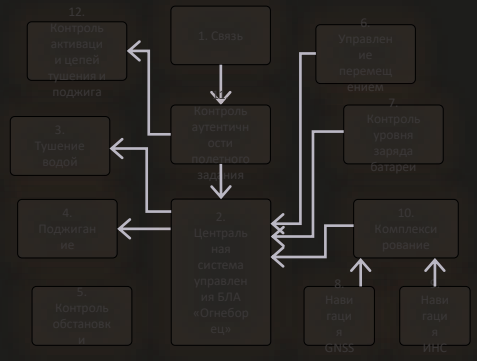
MILS - https://en.wikipedia.org/wiki/Multiple_Independent_Levels_of_Security

Преимущества решений с изоляцией компонент в **µ-ядерной ОС**

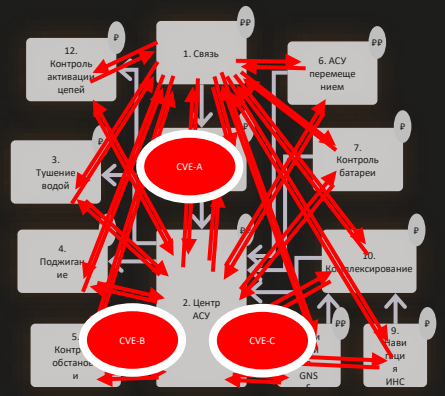
1. Монолитное решение «БПЛА»

2. Декомпозиция решения «БПЛА» 12 на компонент

3. Количество потоков управления в БПЛА = 10



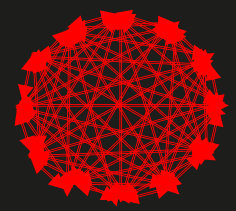
4. Потенциальные направления атаки внутри для 2х компонент



Количество направлений атак внутри ВСЕХ 12 компонентов равно

n*(n-1)=132

5. Сокращение кол-ва направления атак в БПЛА на KasperksyOS



$$\frac{\text{———}}{\text{———}} = \frac{10}{132} < 8\%$$

ВЫВОДЫ

Количество потенциальных уязвимостей (ПУ) в решении декомпозированном на домены безопасности с контролем взаимодействия в решении «БПЛА» составляет менее ПУ=8% от всех в потенциальных типов уязвимостей в монолитном решении

Исследования* показывают, что в общем случае можно ожидать достижения уровня ПУ=40% или роста защищённости >2 раз

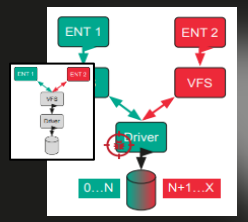
* https://trustworthy.systems/publications/full_text/Biggs_LH_18.pdf

2 Кибериммунный дизайн – безопасность устойчивая к (не)известным угрозам

CYBERIMMUNITY PRINCIPLES

- Secure by Design
- Methodology
- Security models
- Architectural patterns
- Minimizing Trusted Code Base
- Heuristic principles
- Kernel separation
- Security Monitor

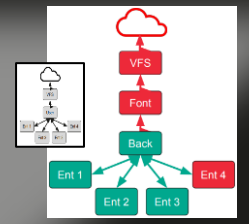
Trustful telemetry pattern



MILS

FLASK

Trustful storage pattern



µ-kernel

TLS Terminator pattern

Secure Logging

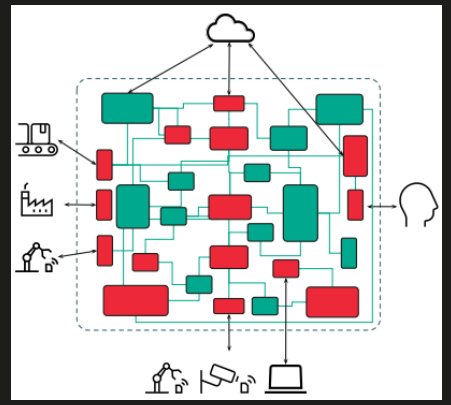
Secure boot & secure update

Resource Manager pattern

Displacement of trust

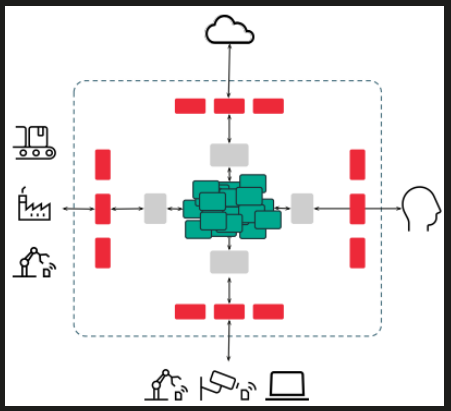
* * *

As-Is



Все кибериммунные практики примененные в решении

To-Be



устойчивость к (не)известным угрозам

Как кибериммунитет снижает сложности защиты системы

Монолитная АСУ БПЛА

Атака на практически любой компонент нарушает цели безопасности

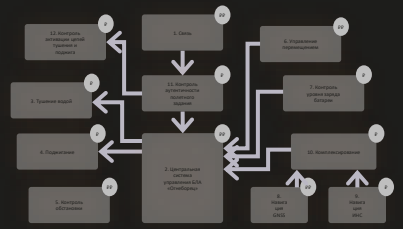
Снижение поверхности атаки

за счет

Разделение решения на независимые домены в MILS среде (μ-ядерной KasperskyOS)

Существенное* снижение сложности защиты

Разделение АСУ на домены безопасности с политиками взаимодействия



Атака на компонент в одном домене безопасности не влияет на компонент в другом домене

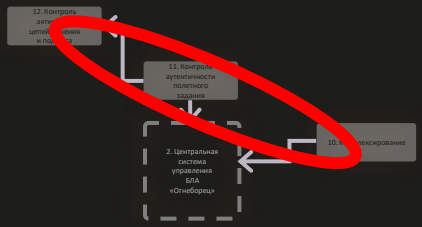
Минимизация поверхности атаки

за счет

Кибериммунного проектирования архитектуры

Дальнейшее снижение сложности защиты**

В кибериммунном проектировании надо защитить только критичных для ИБ компоненты



Не требуется полностью защищать сложные и «важные» компоненты исключая SA/DA/PE тесты для них сокращая далее «цену» безопасности

Снижение сложности защиты на порядок!

** По экспертным оценкам Лаборатории Касперского достигает 2 и более раз*

*** Зависит от архитектуры, целей и предположений безопасности*

3 Кибериммунитет – что же он дает в конце концов?

Природа дала человеку иммунитет от большинства вредных болезней, а Лаборатория Касперского принесла в ИТ кибериммунитет для защиты от большинства киберугроз.

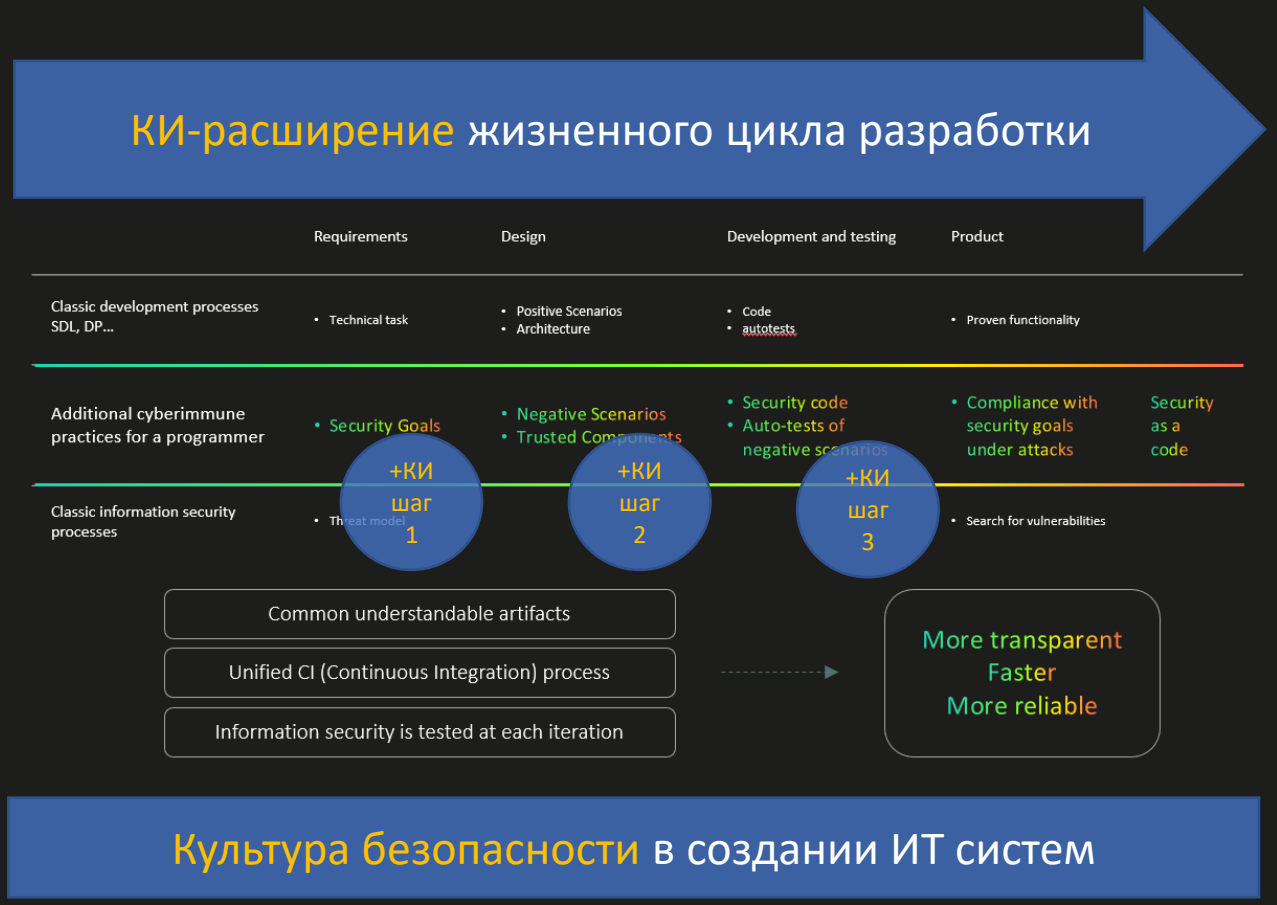
Как с угрозами поступают в других областях

- Пожары в степи тушат встречным палом, который изолирует зону пожара от живых посевов
- Автомобили проектируют разрушиться в ДТП, спасая пассажира изолировав зону разрушения от салона
- Сейсмоустойчвые здания делают не прочными, а разделенными на устойчивые к колебаниям части

В результате – кибериммунитет делит решение на независимые части не давая атаке злоумышленника распространиться с одной на другую, а это позволяет усилить защиту только тех частей решения, которые необходимы для обеспечения целей безопасности в условиях выбранных предположений, что позволяет снизить стоимость защиты

С точки зрения процесса проектирования - кибериммунитет расширение ЖЦ ПО – кодирование безопасности в процессе проектирования (или «безопасность как код»)

- Шаг 1 – включает цели безопасности на основе принятых предположений на этапе анализа требований (что при правильном проектирование исключает сами причины уязвимостей заданных типов)
- Шаг 2 – создание доменов безопасности вместе с функциональными доменами, их изоляцией и контролем взаимодействия посредством политик безопасности (кодирование безопасности в них) предполагаю что какой-то из доменов когда-то может быть взломан.
- Шаг 3 – отрицательные тесты, на защиту от атак. В совокупности это дает решение защищающее от известных и еще неизвестных уязвимостей благодаря своей конструкции.



Как освоить самому
или организовывать обучение кибериммунной разработке

Целевой сегмент – 3й год обучения программиста (to-be видение – все ИТ специальности)

Изоляция ПО на KasperskyOS

КИ-проектирование

PUBLIC SDK & Documentation
https://os.kaspersky.ru/development

OPENSOURCE COMPONENTS
https://os.kaspersky.ru/development/components

TECH SUPPORT FORUM
https://forum.kaspersky.com/forum/kasperskyos-разработка-32/

PROJECT EXAMPLES (opensource)
https://os.kaspersky.ru/development/cases

KASPERSKYOS FUNDAMENTALS
HAL / Boot / Drivers / POSIX / IPC / PSL ...

PATTERNS & RESEARCHES
Functional / Security / Diploma & Research

Methodological materials:

ASIS TOBE

CYBERIMMUNE WIKI
https://github.com/sergey-sobolev/cyberimmune-systems/wiki

CYBERIMMUNITY FOR 3 DAYS (online trainings)
https://www.youtube.com/@learning_cyberimmunity

CYBERIMMUNE GAME
Fire Fighter Drone

ONLINE HACKATHONS
on cyber immune systems development format and materials

CASE STUDIES
for cyber immune systems design with and without solutions

DIPLOMA SUBJECTS
Bachelor projects format description and topics list

Выпускник:
системный программист со знанием кибериммунной работы в KasperskyOS

Необходимы навыки встроенной разработки на C++
и базовые знания в области информационной безопасности

Выпускник:
архитектор ИТ систем широкого профиля

достаточно общее знакомство с программированием
и базовые знания в области информационной безопасности

Nota Bene:

Да, все публично! – По ссылкам выше. Можно изучать прямо сейчас. Не требует никакой авторизации.

Нужна поддержка? – возможна, но при условии обязательных предметов в вузе или открытого кода ваших проектов.

Перспективные исследования кибериммунных технологий

С1. Сравнения технологий

С1.1 Выполнить обзор публично доступных материалов, сопоставляющих микроядерные и монолитные операционные системы. Опубликовать статью с перечнем наиболее подходящих критериев для качественного или количественного сопоставления решений на базе микроядерных и монолитных ОС, с их оценкой/ранжированием.

С1.2 Выбрать наиболее показательные критерии для оценки. Выполнить сравнение микроядерных и монолитных ОС на основе этих критериев. (Смысл этой работы в получении более свежих результатов. Большинство статей, что есть в публичном поле, написаны давно, а мир монолитных систем тоже не стоит на месте. В работе также нужно сослаться на результаты аналогичных статей и показать, что изменилось с тех пор.)

С1.3 Выполнить обзор публично доступных материалов, сопоставляющих ОС с реализацией FLASK-подобного монитора обращений и другие системы. Проанализировать критерии, по которым происходит сравнение. Опубликовать статью с перечнем наиболее подходящих критериев для качественного или количественного сопоставления решений с FLASK-подобным монитором обращений и без него.

С1.4 Выполнить сравнение систем с FLASK-подобным монитором обращений и традиционных ОС, пользуясь критериями, полученными в задаче выше.

Ф2. Формализация характеристик безопасности кибериммунных решений

Ф2.1 В первых продуктах, вышедших на KasperskyOS, использовалась модель контроля целостности, неформально заданная правилами, перечисленными далее по тексту. Для любого кибериммунного продукта необходимо построить формальную модель, использующую язык теории множеств и логики первого порядка. Для примера подобных формальных моделей см. книги Matt Bishop «Computer Security: Art and Science», Петр Девянин «Модели безопасности компьютерных систем», статью Дмитрия Кулагина и Владимира Буренкова «Модель мандатного контроля целостности в операционной системе KasperskyOS».

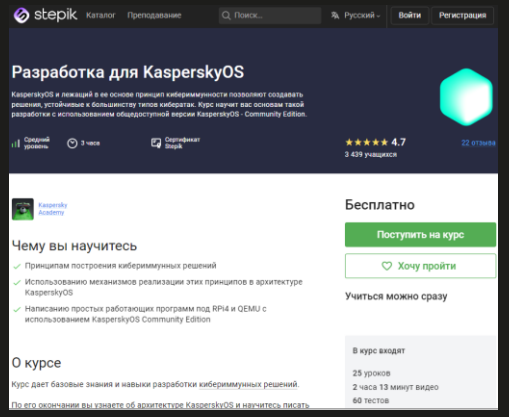
Ф2.2 Ранее опубликованная работа Дмитрия Кулагина и Владимира Буренкова «Модель мандатного контроля целостности в операционной системе KasperskyOS» описывает новую формальную модель контроля целостности, реализация которой доступна в KasperskyOS. Для этой модели доказана теорема, гарантирующая, что при компрометации компонентов с определенным уровнем целостности, часть компонентов (с более высоким уровнем) останется не скомпрометированной. Утверждается, что модель из пункта 5 является подмножеством модели Кулагина-Буренкова. Необходимо формально подтвердить эти догадки (или опровергнуть, если это не так).

М3. Оценка реализации моделей безопасности современных мобильных платформ

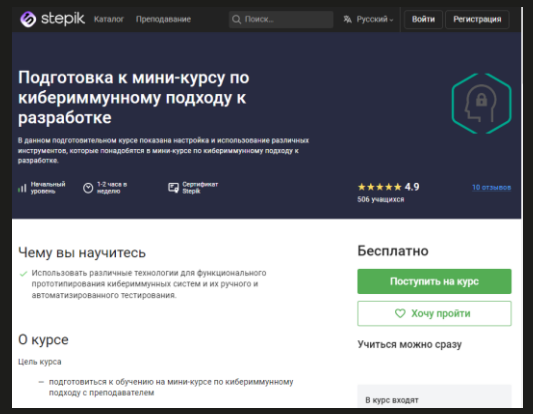
М3.1 На сегодняшний день Android, iOS/iPadOS и ChromeOS являются наиболее продуманными в плане безопасности популярным операционными системами общего назначения. Модель безопасности ОС Android хорошо продумана и многократно описана в публикациях. Угрозы из модели угроз Android митигируются различными средствами, предоставляемыми ядром Linux или модификациями, добавляемыми разработчиками ОС Android. Часто эти митигации выглядят, как "костыли", например, построение песочниц (sandboxes) на основе Unix DAC и MAC, или IPC, построенное на основе Android binder и плохо интегрированное с остальным Unix-миром. Когда мы пытаемся митигировать те же угрозы средствами микроядерной ОС KasperskyOS, становится очевидно, что митигации естественно реализуются за счет базовых механизмов системы, без необходимости обходиться плохо подходящими инструментами. Например, sandboxes реализуются "из коробки", т.к. по умолчанию ни один процесс не имеет доступа к каким-либо сервисам в системе, в т.ч. ядерным, пока это явно не будет прописано в политике безопасности, или не будет передан ОСАР-хендл на объект. Android binder имитирует возможности, которые предоставляются любой современной микроядерной ОС, причем возможности по удаленной работе с объектами в таких системах лежат в самой их основе, а не "приделываются" сбоку. Предлагается пройтись по модели угроз Android и взамен описанных в статьях митигаций предложить решения, которые были бы естественными на KasperskyOS и других подобных системах. Результаты опубликовать в виде рецензируемой статьи.

Популяризация технологий - Курсы, Хакатоны, Дипломы, …

https://t.me/+lVB5cjMoeisyYzdi



https://stepik.org/course/73418/promo

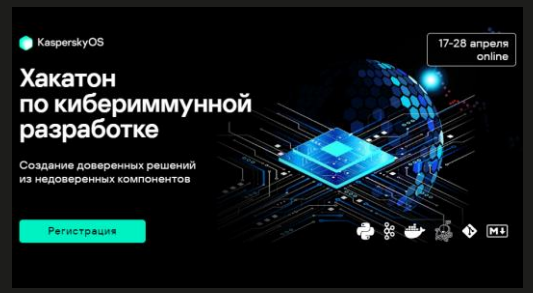


https://stepik.org/course/133991/promo

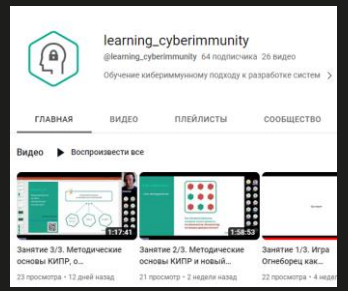
https://t.me/learning_cyberimmunity

https://os.kaspersky.ru/latest/hackathon-mai-kasperskyos/

https://mai.ru/press/news/detail.php?ID=175115&referer=https%3A%2F%2Fwww.google.com%2F



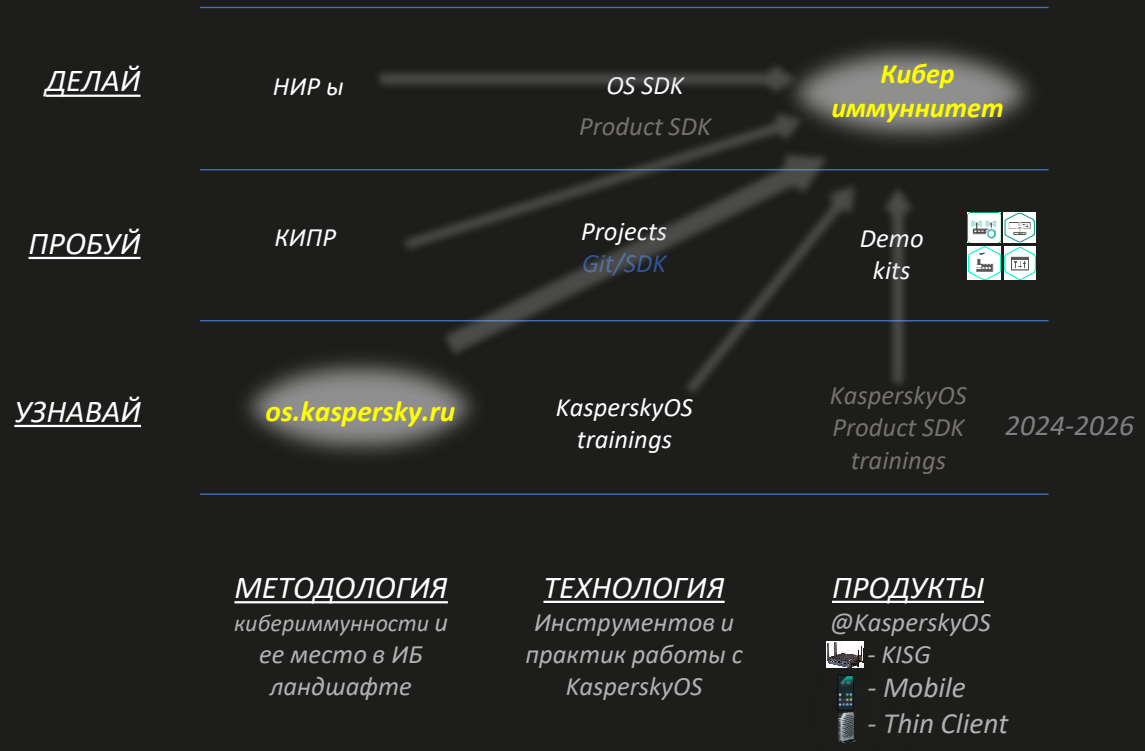
https://hackathon-cyberimmune.ru/



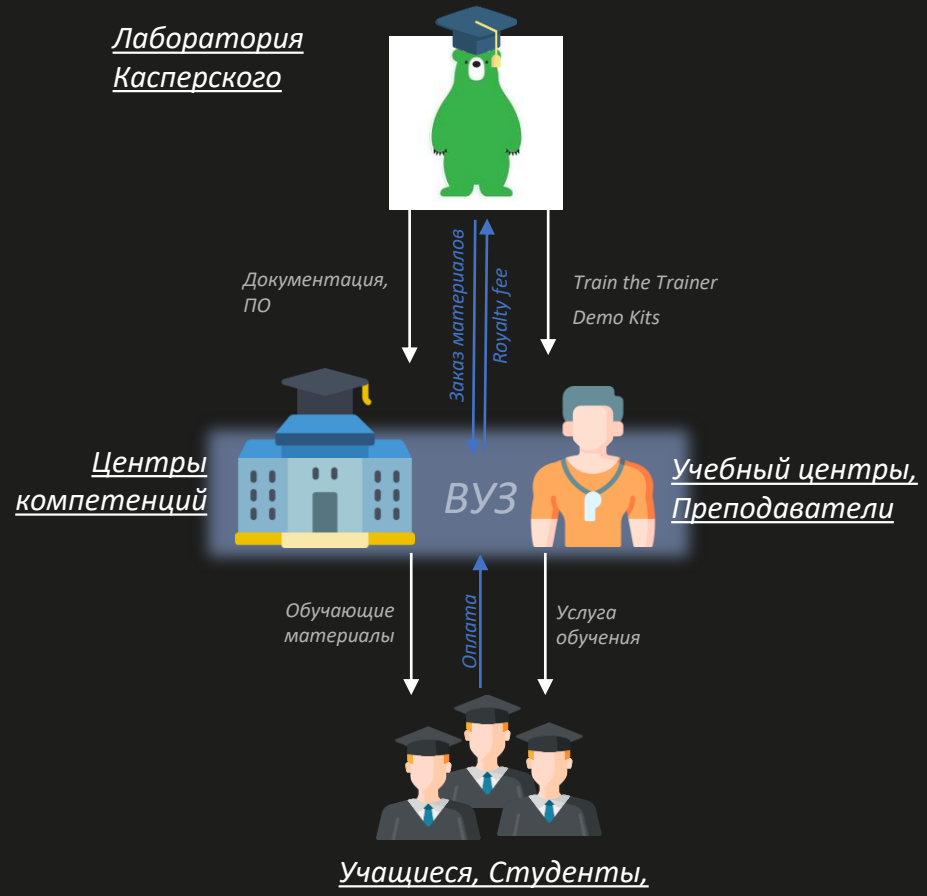
https://www.youtube.com/@learning_cyberimmunity

Предложение для академический партнеров на 2024-2026

Инициативы ЛК по продвижению кибериммунитета на рынок



Видение взаимовыгодного развития кибериммунных образовательных продуктов



Следующие шаги подготовки ИТ-шников кибериммунитету:

- ✓ Изучать методологию кибериммунного проектирования
  - Изучать МЕТОДОЛОГИЮ КИПР и обучать ей студентов как новой ИБ дисциплине (курсы/дипломы)
  - Сравнивать/формализовывать кибериммунные техники с ППС (консультации/исследования/рецензии)
- ✓ Создавать ИТ технологии на изолированных доменах в KasperskyOS
  - Обучать новой ИНЖЕНЕРНОЙ дисциплине (курсы/дипломы/проекты) работы с KasperskyOS
  - Обучать созданию бизнес приложений кибериммунных платформ
- ✓ Развивать кибериммунные продукты совместно с лидерами рынка
  - Тестировать и интегрировать лучшие кибериммунные решения
  - Осваивать SDK от лидеров кибериммунной разработки

Спасибо!

KasperskyOS