KAZAKH KBTU BRITISH
TECHNICAL
UNIVERSITY

«Подготовки кадров в сфере информационной и кибербезопасности на основе практических бизнес-кейсов»

Байтасов Калилалло Маркисович

к.э.н., академик МАИН, член экспертного совета МОАП РК по кибербезопасности,

Руководитель лаборатории кибербезопасности АО КБТУ

Преамбула

80%

80% cybersecurity risks are low people's knowleg&expirience

600 billions $

The global damage from cyber crime in 2018 amounted to more than 600 billion dollars.

KZ

Kaspersky Lab experts include Kazakhstan in the top 25 most attacked countries in the world

>100 K

The growth of computer incidents in 2017 - more than 100 thousand.

- Мировой ущерб от каиберпреступности в 2018 году составил более 600 миллиардов долларов.
- Казахстан привлекает все большее внимание киберпреступников (входит в ТОП-20), в связи с развитием своей экономики, но недостаточным развитием системы противодействия им. И хотя в стране предпринимаются усилия по борьбе с новыми угрозами, однако делать акцент только на аппаратно-технические средства противодействия не соврем правильно, ибо упускаются экономические, социальные и правовые аспекты.
- Как известно почти 80% кибератак в мире стали возможны «благодаря» человеческому фактору: «простые пароли», пароли записанные на бумагу, несменяемость паролей пользователей, передача паролей третьим лицам, один пароль для нескольких сервисов и прочее.

Концепция современного центра обучения КБ

Коротко об лаборатории

КБТУ 14 декабря 2017 года стал полноправным участником консорциума по кибербезопасности с Комитетом информационной безопасности МОАП РК.
В сентябре 2018 года открыта лаборатория кибербезопасности АО «КБТУ».
В 2018 году проведены работы:

•Заключен меморандум о сотрудничестве с Лабораторией Касперского и лицензионный договор с Positive Technology

• Совместно с компанией Huawei запущен проект подготовки и сертификации кадров «HCNA- cybersecurity» на базе лаборатории Huawei

• Разработан специализированный курс «Современные технологии информационной и кибербезопасности» (обучено 130 студентов).

• Сотрудники прошли обучение по программе «Лаборатория Касперского для вузов РК» (4 чел)

• Запущен портал по вопросам кибербезопасности, в перспективе он-лайн система обучения

• Выступление с докладом на российской Технологической конференции «Подключенное производство: процессы, активы, люди», проводимая подразделением Хоневелл «Промышленная автоматизация» (HPS) 18-21 сентября 2018 г.

• Участие в международном форуме Astana Digital bridge и выставке проектов Astana Hub Battle, а также участие в выставке проектов Almaty Tech Garden

• Участие в международном конкурсе инновационных проектов «Quality innovation of the year»

•14 июня 2019 НПК «Современные технологии кибербезопасности» (АО КБТУ)

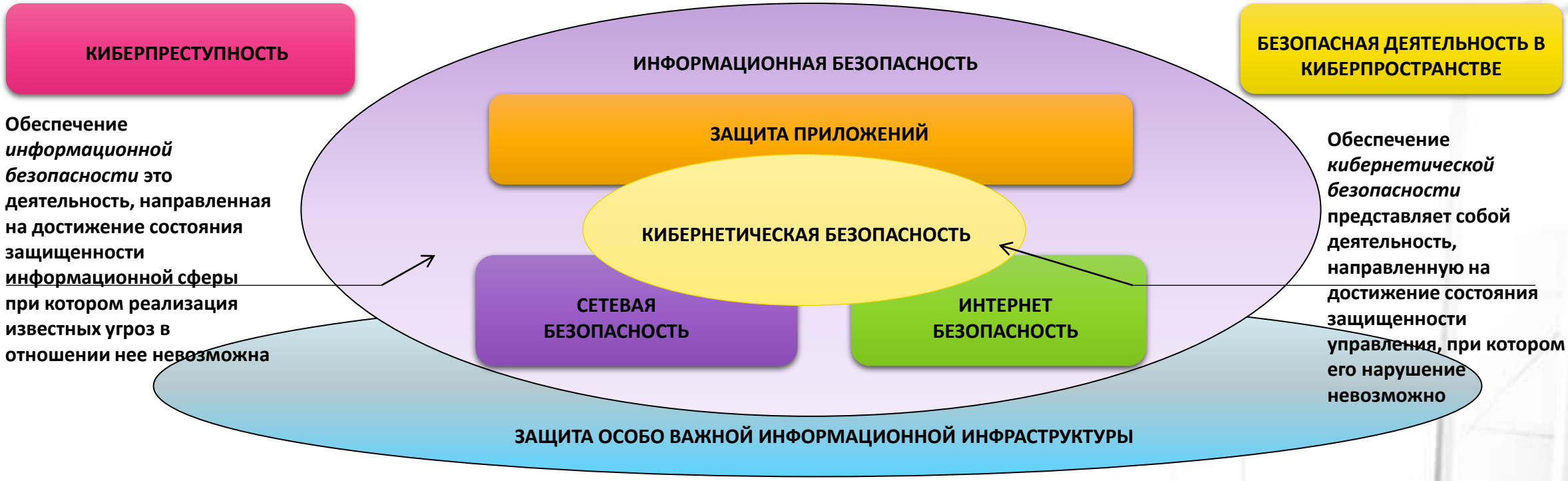
Синергетический эффект

ВУЗ	Технологический партнер
• Получение центра компетенции • Повышения уровня компетенции сотрудников, преподавателей и студентов • Повышения уровня своих корпоративных систем • Возможность использования передовых технологий • Подготовка востребованных рынком выпускников • Привлечение новых клиентов на востребованную услугу – формирование спроса • Создание и использование реальных бизнес-кейсов в учебном процессе	• Получение площадки для продвижения технологий в среде потенциальных специалистов по внедрению и сопровождению продуктов вендора • Получение реальной площадки для «технических туров» • Возможность тестирования и реализации пилотных проектов • Формирования пула экспертов по интеграции или сопровождению продуктов вендора • Элемент социальной ответственности бизнеса – повышение грамотности населения в сфере ИКБ, поддержка перспективной молодежи и прочее • Реальный и репрезентативный объект для реализации маркетинговых мероприятий • Площадка для отбора перспективных кадров • Пропаганда корпоративных стандартов и перспективных технологий

Учебный курс «Современные технологии информационной и кибербезопасности»

Недели	Аудиторные занятия			
	Тема лекционного занятия	Тема практического занятия	Кол-во часов лекции	Кол-во часов практики
1	Вводная лекция. Общий план курса. Основы информационной и кибербезопасности	Термины и определения. Тренды.	2	2
2	Социальные и правовые аспекты кибербезопасности	Нормативная база. Социально-экономические аспекты в киберпространстве	2	2
3	Системы антивирусной и антиспам защиты: от теории к практике	Основы корпоративной безопасности. Он-лайн практикум на стенде вендора.	2	2
5	Программно-аппаратные системы обеспечения информационной безопасности	Развитие технологий кибербезопасности Практикум на стенде – Безопасный город	2	2
6	Комплексная зашита информации на предприятии	Стандарты и регламенты	2	2
7	Корпоративные сервисы кибербезопасности от ИТ провайдеров	Практикум на стенде поставщика ИТ услуг. Безопасность сетевой инфраструктуры, безопасность ЦОД	2	2
8	Аудит корпоративной системы информационной безопасности	Бизнес-кейс вендора	2	2
9	Системы кибербезопасности промышленных АСУТП	Бизнес-кейс вендора	2	2
10	Бизнес-кейс «Комплексная система кибербезопасности корпорации»	Защита студенческого проекта	2	2
11	ИТОГО		20	20

Соотношение понятий информационной и кибернетической безопасности



Обеспечение *информационной безопасности* это деятельность, направленная на достижение состояния защищенности информационной сферы при котором реализация известных угроз в отношении нее невозможна

Обеспечение *кибернетической безопасности* представляет собой деятельность, направленную на достижение состояния защищенности управления, при котором его нарушение невозможно

ОСНОВНЫЕ ОБЪЕКТЫ ВОЗДЕЙСТВИЯ ИНФОРМАЦИОННО-УДАРНЫХ ГРУППИРОВОК СИЛ И СРЕДСТВ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

- программное и информационное обеспечение
- программно-аппаратные, телекоммуникационные и другие средства информации и управления
- каналы связи, обеспечивающие циркуляцию информационных потоков и интеграцию системы управления
- информационные сервисы обеспечивающие бизнес-процессы

IBM X-Force Threat Intelligence Index 2017

Sampling of security incidents by attack type, time and impact, 2014 through 2016

Size of circle estimates relative impact of incident in terms of cost to business, based on publicly disclosed information regarding leaked records and financial losses.

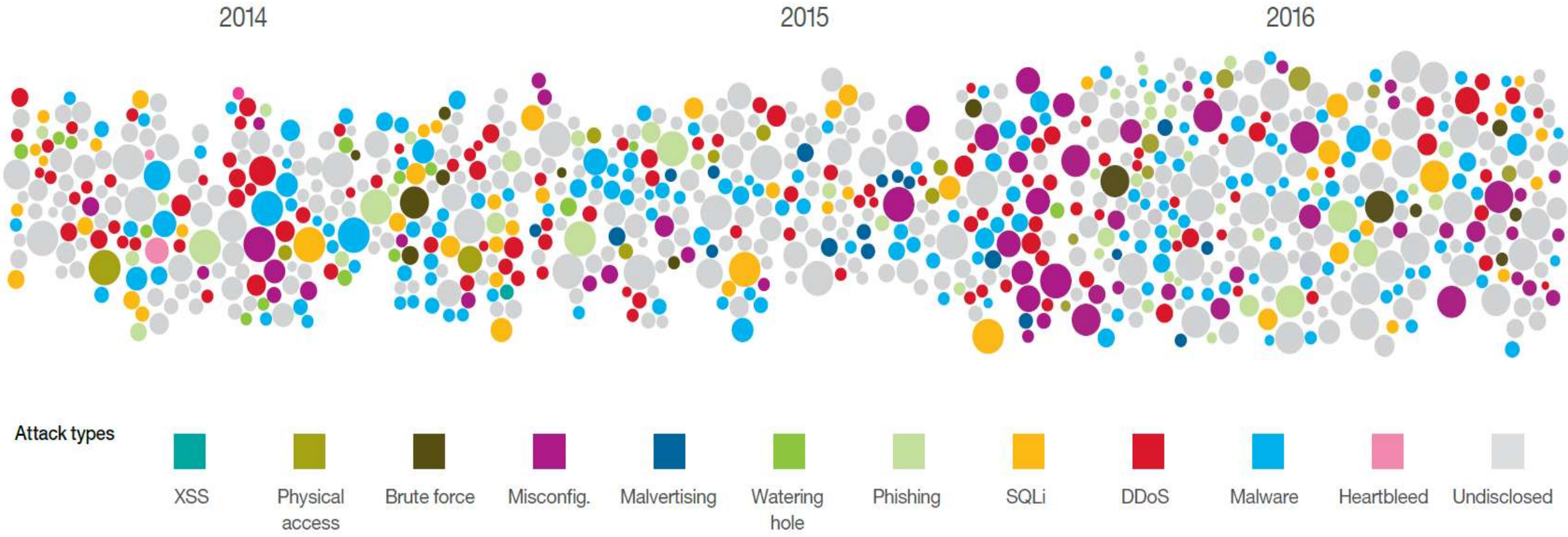


Figure 3: Sampling of security incidents by attack type, time and impact, 2014 through 2016.

Тренды кибербезопасности до 2025 года

Защита от DDoS-атак.

Количество атак будет расти, т.к. падает стоимость самой атаки + широкое распространение IoT

Защита малого и среднего бизнеса от типовых атак

Существенное увеличение количества атак на малый и средний бизнес за счет низкого уровня защищенности таких компаний

Защита от таргетированных атак

Если раньше основной целью APT-атак был в основном саботаж или кибершпионаж, то теперь этот инструмент все чаще используется и непосредственно для обогащения злоумышленников. Атаки дешевеют и не требуют высококвалифицированных компетенций

Безопасность BYOD

Повышение количества личных устройств сотрудников, используемых для работы

Повышение числа предприятий, предоставляющих сотрудникам смартфоны и планшеты для корпоративных нужд

Информационная безопасность как сервис

Экономический эффект и выгода. Компании начинают формировать стратегию и считать риски, отдавая функцию ИТ\ИБ в аутсорсинг.

Повышение культуры кибербезопасности

Воспитание гражданского общества, концепция дома – гражданин, на работе – сотрудник. Цифровая гигиена должна быть на всех слоях жизни

Безопасность АСУ ТП\IIoT\IoT

Повышение уровня автоматизации повышение производительности, снижение влияния человеческого фактора, оптимизация процессов, доступ к данным для анализа трендов. Стандартные IT платформы Windows, SAP, и TCP/IP являются новыми стандартными платформами для контроля процессов

Искусственный интеллект (Big Data, ML, UBA, AI)

Предсказание и предотвращение проблемы до того, как она произошла

В условиях кризиса выгоднее наращивать не количество ИТ- и ИБ-систем, а модернизировать функционал уже существующих, в том числе – посредством ввода аналитических инструментов.

Комплексный подход при построении КСЗИ

Межсетевые экраны
Trust Access
Check Point
Cisco FWSM, ASA
StoneGate FW
PaloAlto

Средства обнаружения вторжений
Check Point IPS
Cisco IPS
StoneGate IPS
IBM ISS Proventia
SSEP HIPS

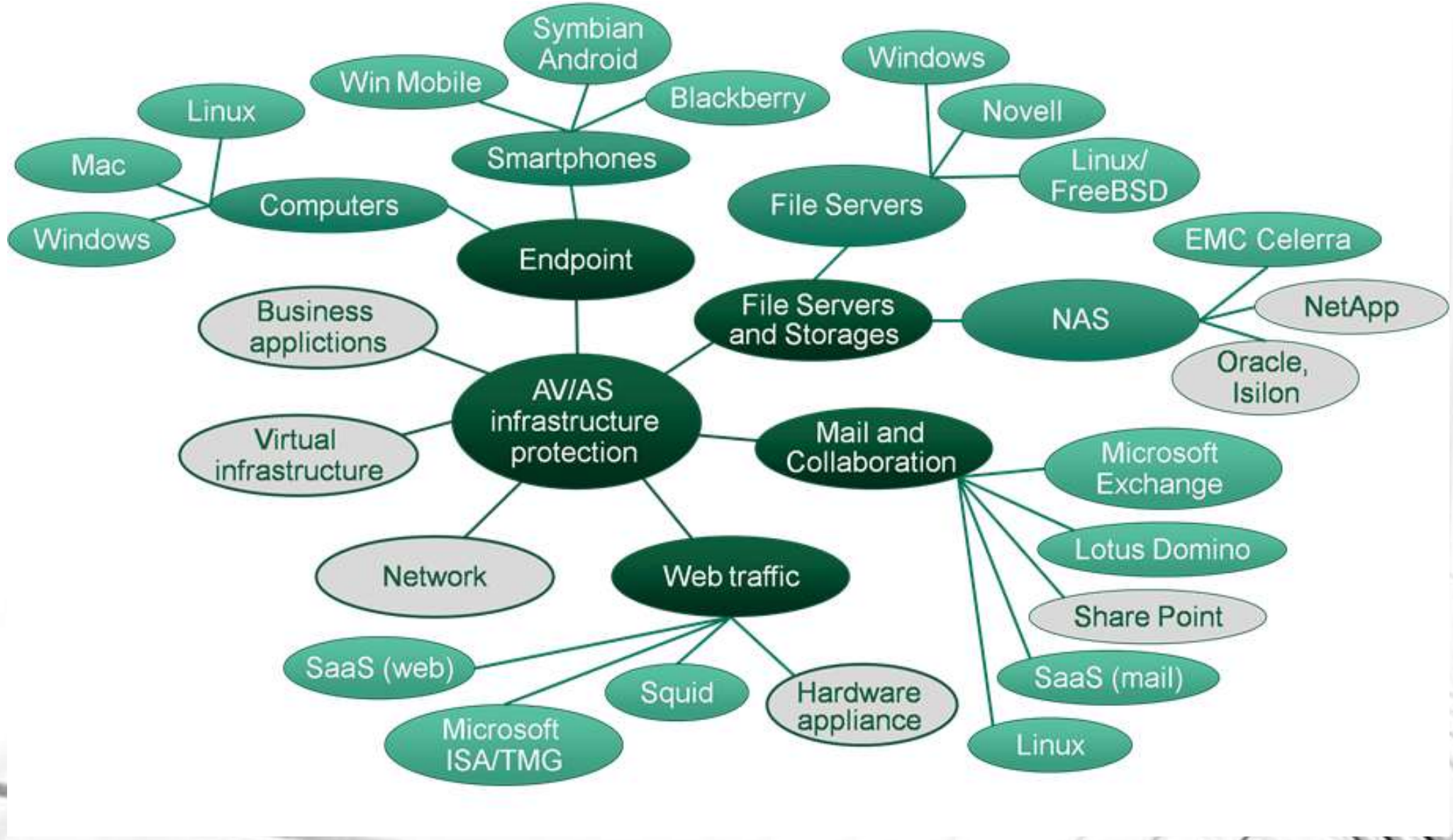
Защита от НСД
Secret Net
vGate

Анализ защищенности
MaxPatrol
XSpider

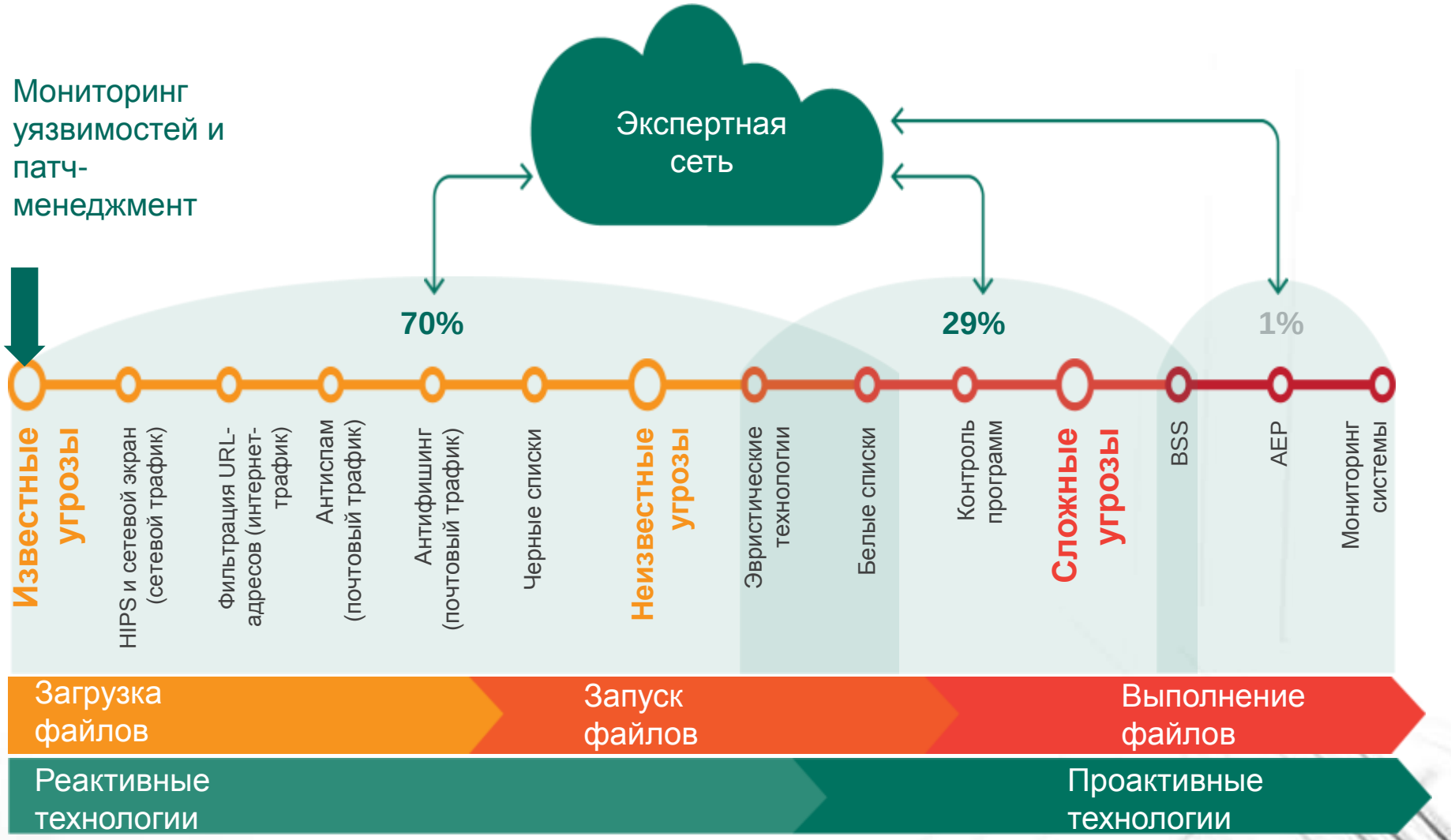
Защита каналов связи
StoneGate SSL
ViPNet

Сервисы «физической защиты»
СКД,
Access Control System,
Abra, VDC

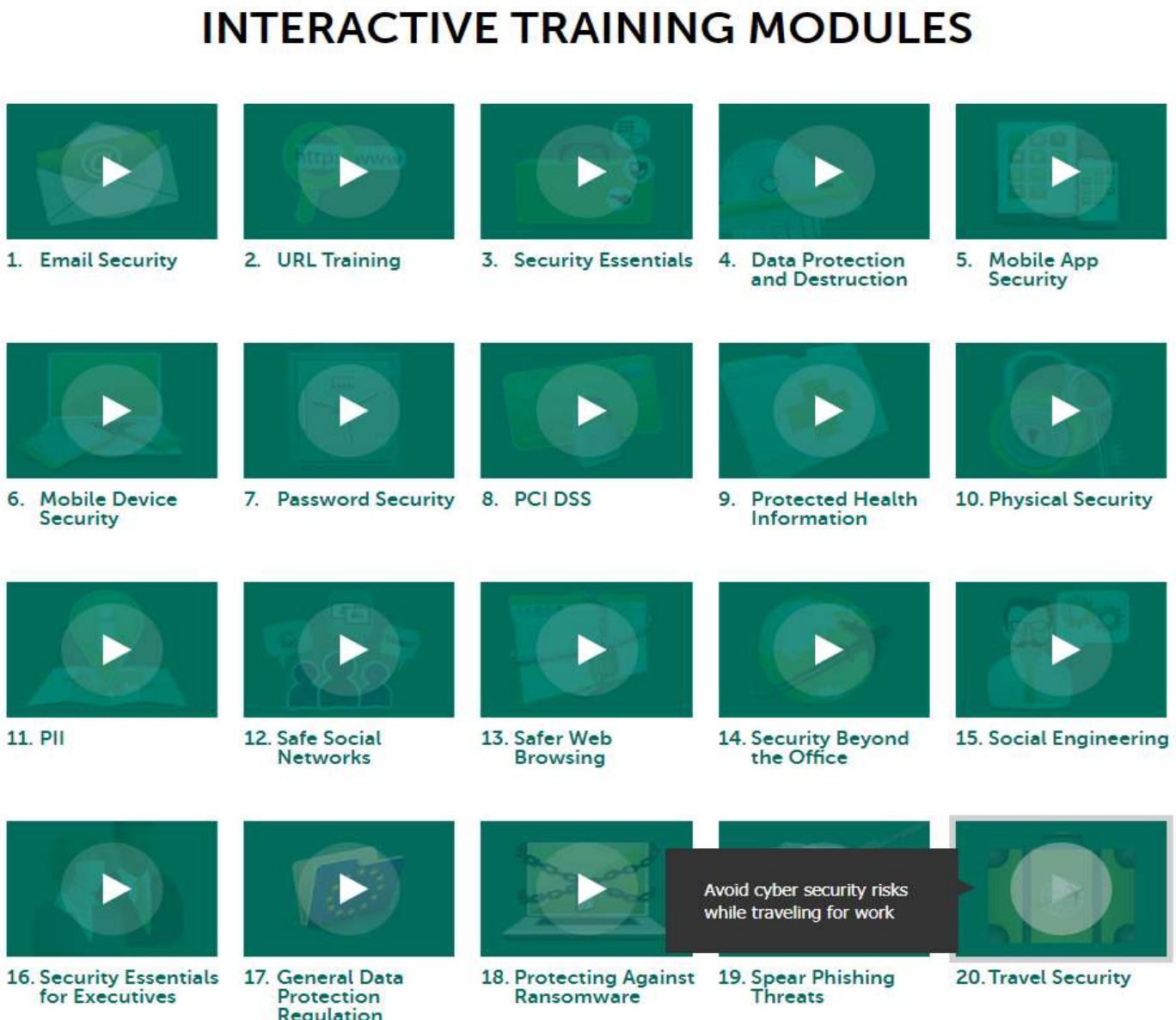
Комплексный подход к антивирусной и антиспам защите



Единая платформа кибербезопасности



Он-лайн система практических занятий



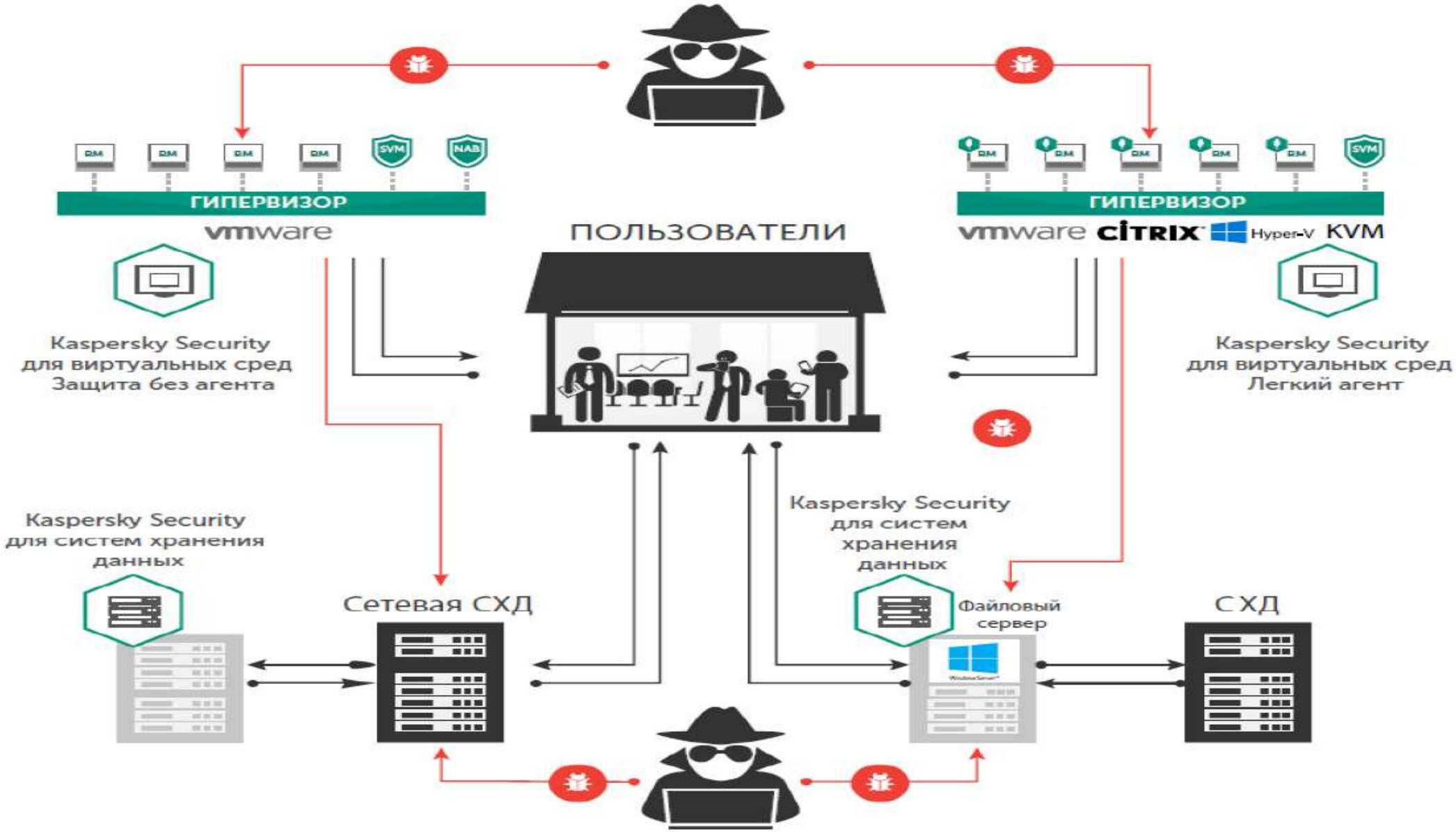
Программа повышения осведомленности

«Лаборатория Касперского» предлагает тренинги по информационной безопасности для сотрудников всех уровней. В них используются игровой подход, практические занятия, имитация атак и другие интерактивные методики. Это позволяет формировать устойчивые привычки и укреплять кибербезопасность в долгосрочной перспективе. Большинство тренингов проходят в онлайн-формате, что позволяет легко отслеживать успеваемость пользователей и контролировать ход обучения.

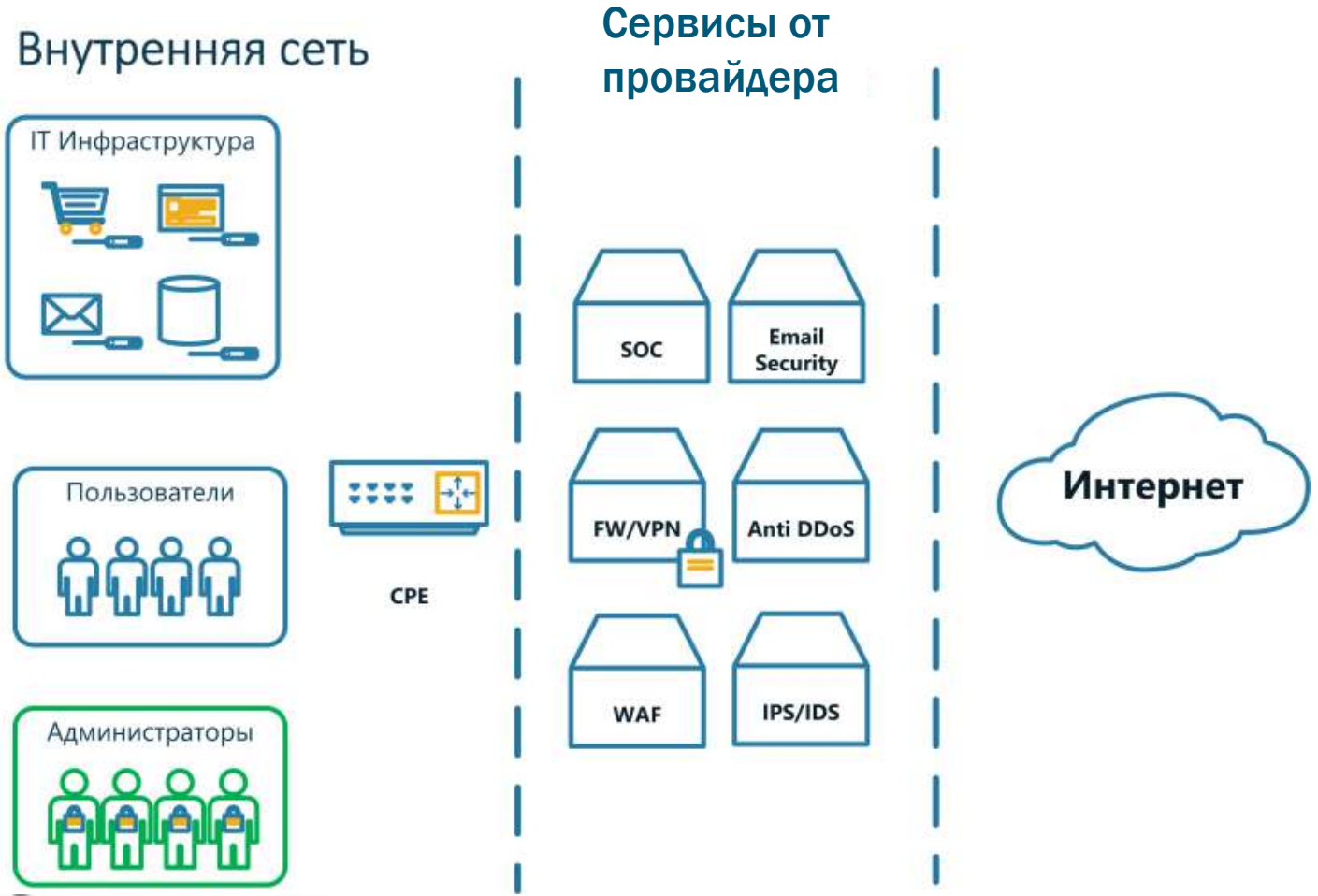
Практикум
«Защита критической инфраструктуры предприятия»

- Защищать производственные предприятия от киберугроз
- Обеспечивать безопасность промышленных сред и непрерывность производственных процессов
- Минимизировать время простоев и задержки технологических процессов
- Расследование инцидентов

Практикум «Защита корпоративного ЦОД»



Сервисная модель построения системы защиты информации



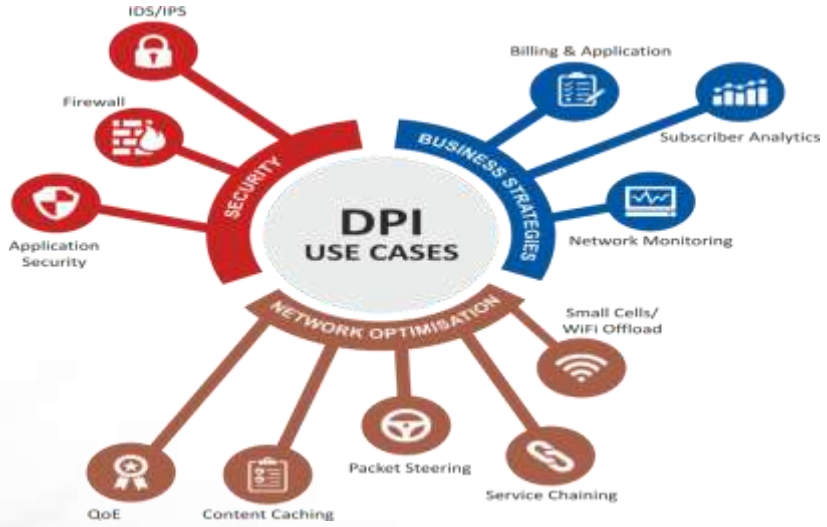
- ✓ Гибкость конфигурации и
- ✓ Возможность быстрого наращивания или сокращения мощностей
- ✓ Единое окно управления всеми СЗИ
- ✓ Эксплуатация системы защиты силами квалифицированных специалистов
- ✓ Мониторинг и реагирование на инциденты ИБ в режиме 24x7
- ✓ Отсутствует необходимость в большом штате дорогостоящих инженеров ИБ
- ✓ Форма затрат – OPEX

Бизнес кейс
«Безопасные корпоративные сервисы ИТ провайдера»

Защита от DDoS атак

Облачное видеонаблюдение

DPI (Deep Packet Inspection)



Облачная ИТ инфраструктура

Бизнес кейс «Безопасный город»

① Единый командный центр

Прием обращений

Диспетчеры

ICP/IoT

Видео консультации

⑤ Системы Big-data

Социальные сети

Цифровая криминалистика

Платформа Big-data

⑨ Управление

eSight

eOMC

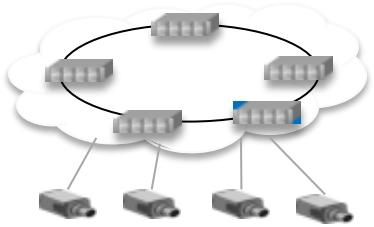
⑩ Сервис

Проектирование

Внедрение

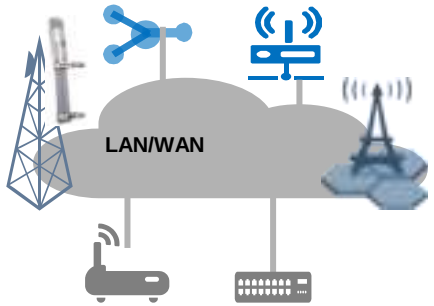
Поддержка

②Интеллектуальное видео



VMS

VCM



⑦ Agile NetConnect

④ Транспортная безопасность

Контрольные точки

E-Police

Дорожное видеонаблюдение

Мультимедийная коммуникация

eLTE Rapid

ECV

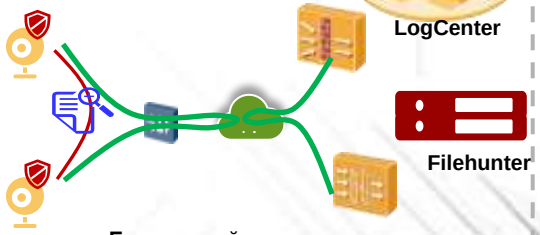
③ Оперативная коммуникация

⑥ Облачный дата-центр

Распределенный облачный ЦОД

Инфраструктура ЦОД

⑧Инфобезпоасность

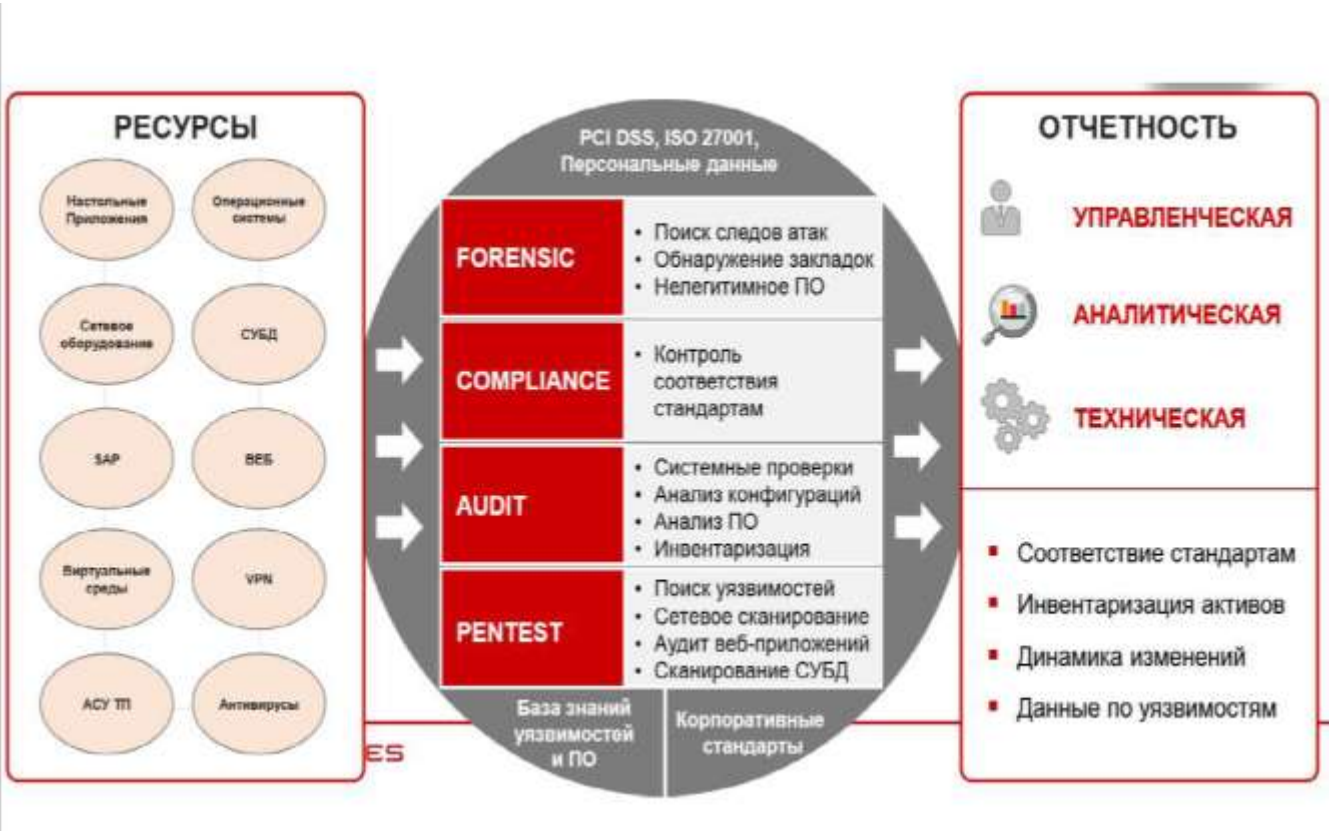


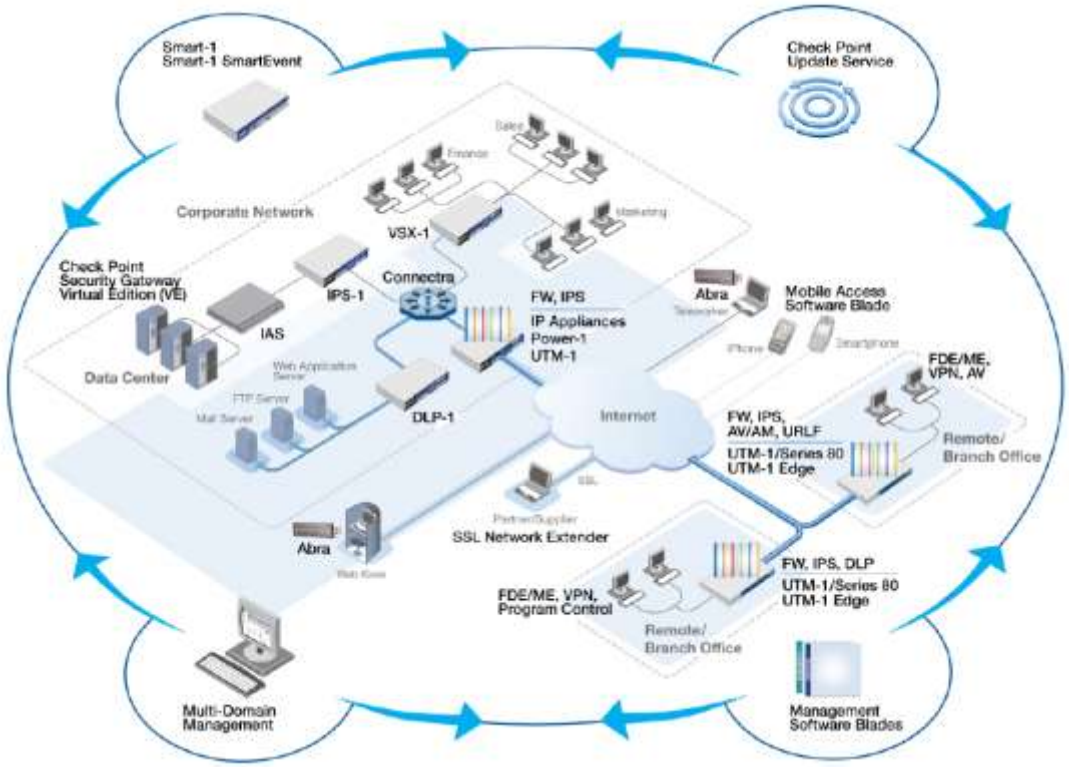
LogCenter

Filehunter

Безопасный доступ

Практикум «Информационный аудит и построение комплексной системы информационной и кибербезопасности»





Перспективы развития

- Создание и развитие совместного с вендорами киберполигона
- Формирование практически ориентированных учебных программ (бакалавры, магистры)
- Он-лайн обучение
- Формирование пула экспертов и студенческих проектных групп
- Создание специализированных учебных программ (МБА, ДБА)

KAZAKH KBTU BRITISH
TECHNICAL
UNIVERSITY

Спасибо за внимание!

Байтасов Калилалло Маркисович

к.э.н., академик МАИН, член экспертного совета МОАП РК
по кибербезопасности
Руководитель лаборатории кибербезопасности АО КБТУ
+7 705 2632694
k.baitasov@kbtu.kz