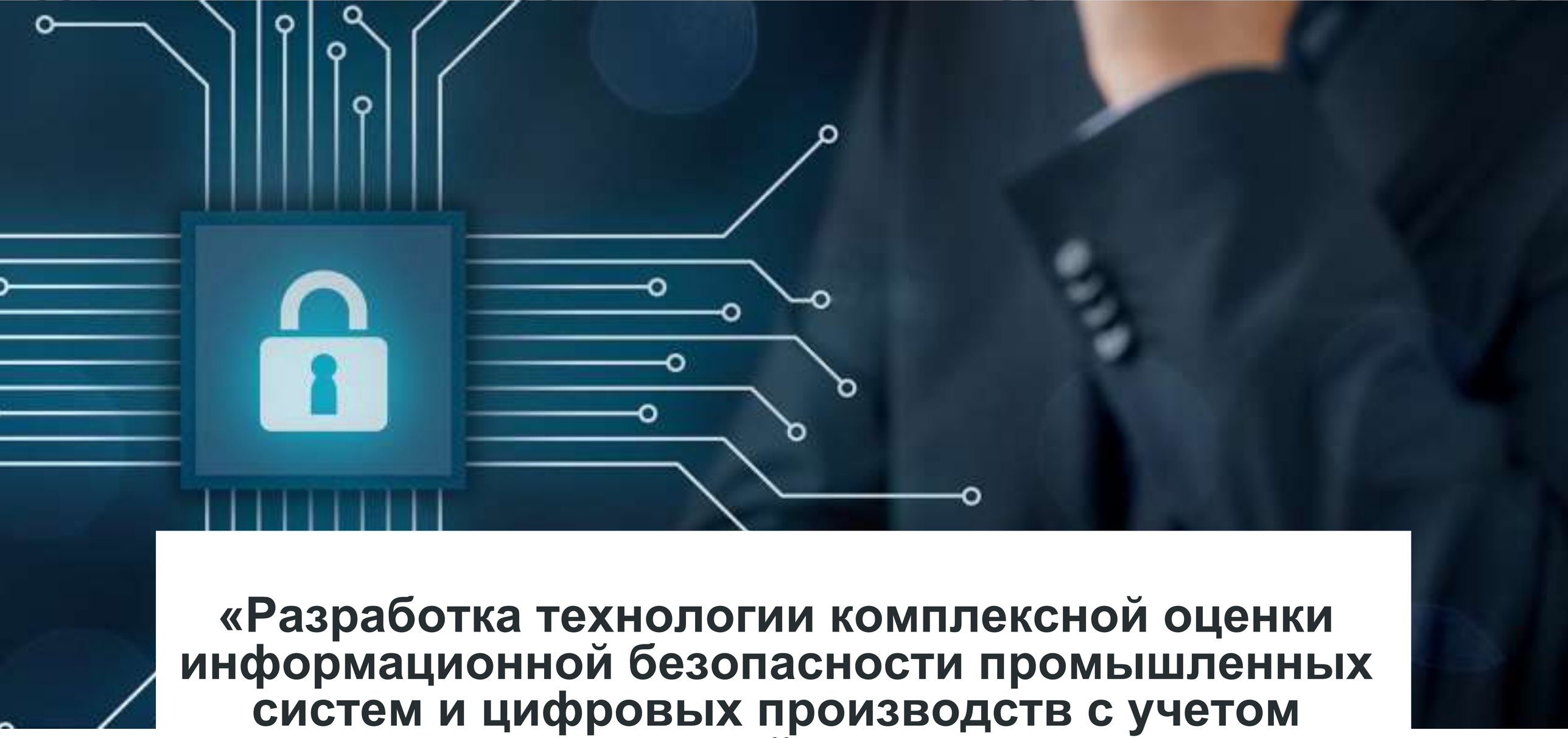


«Разработка технологии комплексной оценки информационной безопасности промышленных систем и цифровых производств с учетом конкретной отрасли»

Филиппов Николай

Актуальность

Количество SCADA-систем, подключенных к Сети без соответствующих мер безопасности, продолжает увеличиваться, что делает критически важные устройства промышленных систем уязвимыми к потенциальным атакам и попыткам взлома. Смягчение последствий кибер-инцидентов теперь требует специальных, а иногда и внешних, дорогостоящих ресурсов. В то же время руководство промышленных предприятий все чаще требует более современной кибербезопасности, поскольку становится яснее, как часто компании подвергаются атакам и во что может обойтись кибер-атака. Как отметили эксперты, более 70% уязвимостей, опубликованных NVD, можно эксплуатировать удаленно. Кроме того, наиболее частым потенциальным воздействием было удаленное выполнение кода, возможное путем эксплуатации 49% уязвимостей, за которым следует чтение данных приложений (41%), вызов отказа в обслуживании (39%) и обход механизмов защиты (37%). Стоит отметить, что, хотя фактические инциденты безопасности остались на базовом уровне, и несмотря на сокращение разрыва в кадрах, более половины респондентов (56%) говорят, что нехватка специалистов в области кибербезопасности ставит под угрозу их организации. Учитывая, что экспертов по промышленной кибербезопасности с достаточным опытом в сфере автоматических систем управления технологическим процессом (АСУ ТП) найти непросто и обращение к внешним поставщикам услуг безопасности требует много ресурсов, этот вопрос приобретает особенную важность: если ни наём, ни обращение к сторонним поставщикам невозможны, компании оказываются в практически безвыходном положении. Очевидна важность информационной безопасности для цифровой трансформации.

Предлагаемое решение

Данная технология позволит выявлять уязвимые места в промышленных системах, а также позволит уменьшить проблему, связанную с нехваткой опытных экспертов по промышленной кибербезопасности с достаточным опытом в сфере автоматизированных систем управления технологическим процессом (АСУ ТП). Благодаря предлагаемой разработке возможно сократить количество экспертов, которые на сегодняшний день необходимы для оценки рисков и уязвимостей в системах.

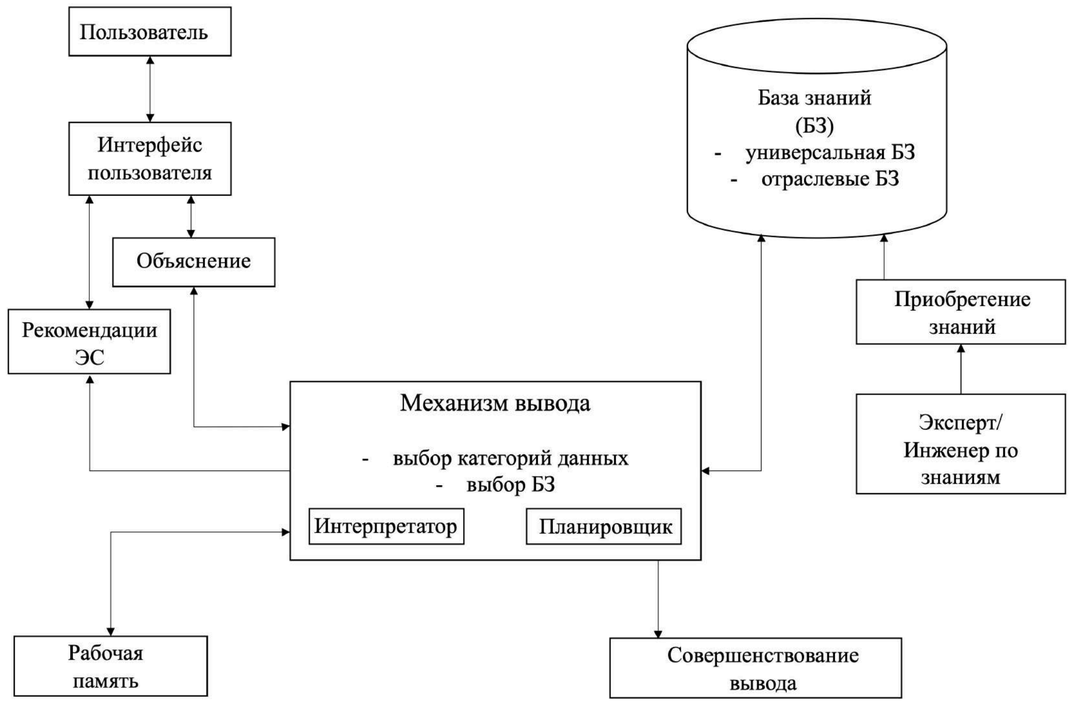
Научная новизна проекта

Технология комплексной оценки информационной безопасности промышленных систем и цифрового производства с учетом конкретной отрасли состоит из:

1. Методика наполнения внутренней базы знаний экспертной системы;

2. Алгоритм взаимодействия пользователя и информационной системы, который позволяет при необходимости выделить составляющую для конкретной отрасли в процессе оценки информационной безопасности;

3.Метод обнаружения вторжений на основе статистических характеристик трафика.



Сравнение с конкурентами

В качестве конкурентов выделаются: различные решения по защите от вредоносного ПО и антивирусы, средства защиты приложений, мониторинг сети и анализ журналов, сегментация сети, системы обнаружения вторжений. Метод «воздушного зазора» – исключение всякой связи между сетью промышленных систем и традиционной IT-сетью, а также интернетом. Методика vsRisk Risk Assessment Tool, Citicus ONE vR3.2, Lightwave Security SecureAware v3.7.2, Proteus Enterprice и многие другие.

Сравнивая с существующими способами/мерами по обеспечению кибербезопасности промышленных систем предлагаемое решение будет выгодно отличаться большим количество плюсов, одним из них будет возможность использования предлагаемого решения в комбинации с фундаментальными мерами защиты. Не менее важным плюсом, которым будет обладать данная технология, является мониторинг уязвимости с постоянной периодичностью. Более того, проверки будут охватывать не только традиционные IT-компоненты, такие как операционная система для SCADA, а также должна распространяться на конкретные элементы промышленных систем.

Бизнес - модель

ПАРТНЕРЫ

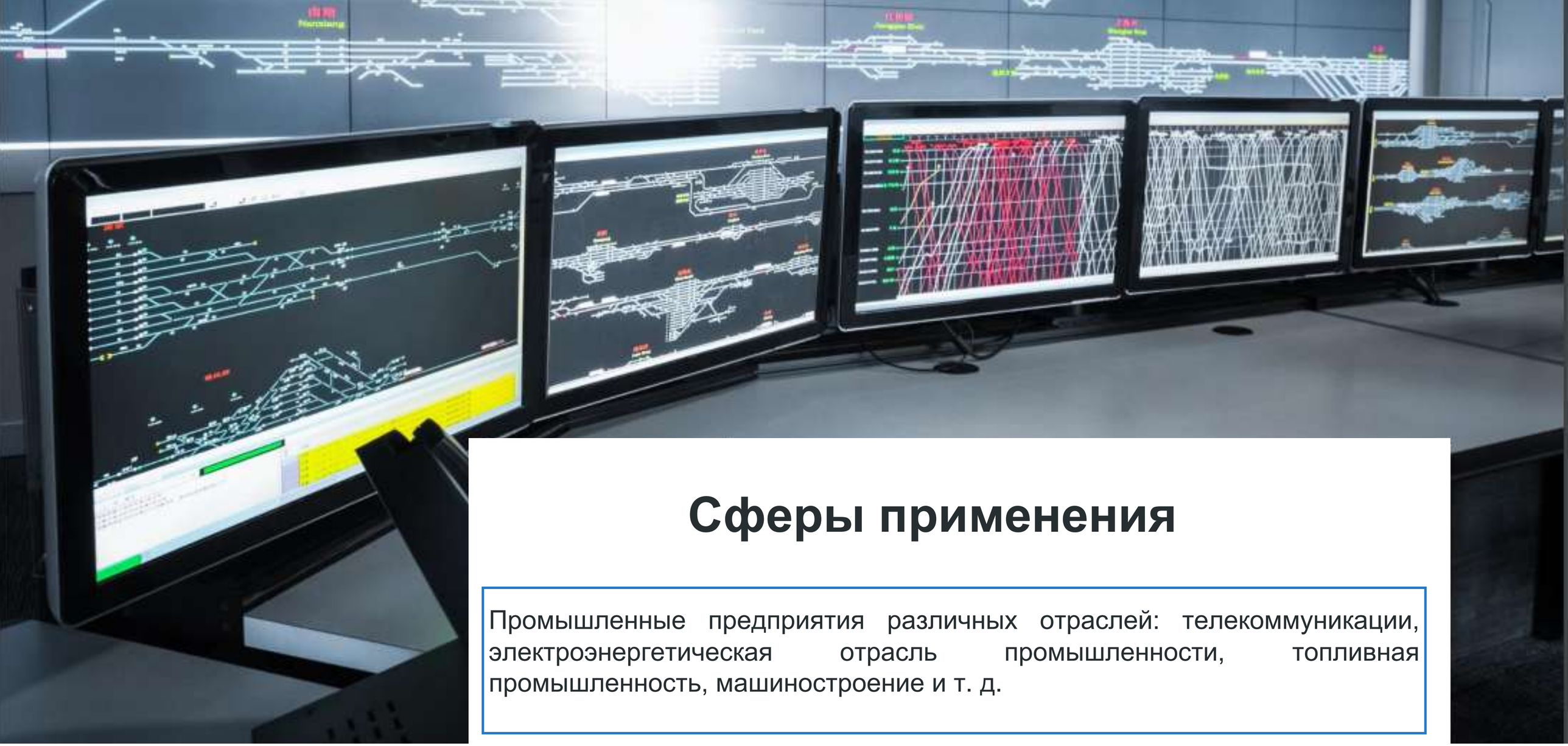
ПГУТИ Кафедра информационной безопасности

ЦЕННОСТНОЕ ПРЕДЛОЖЕНИЕ

Технология позволит выявлять уязвимые места в промышленных системах и цифровом производстве, а также позволит уменьшить проблему связанную с нехваткой опытных специалистов по информационной безопасности промышленных систем, так как благодаря ей возможно сократить их количество.

ПРОДАЖИ

На сегодняшний день планируется продажа технологии крупному игроку на рынке

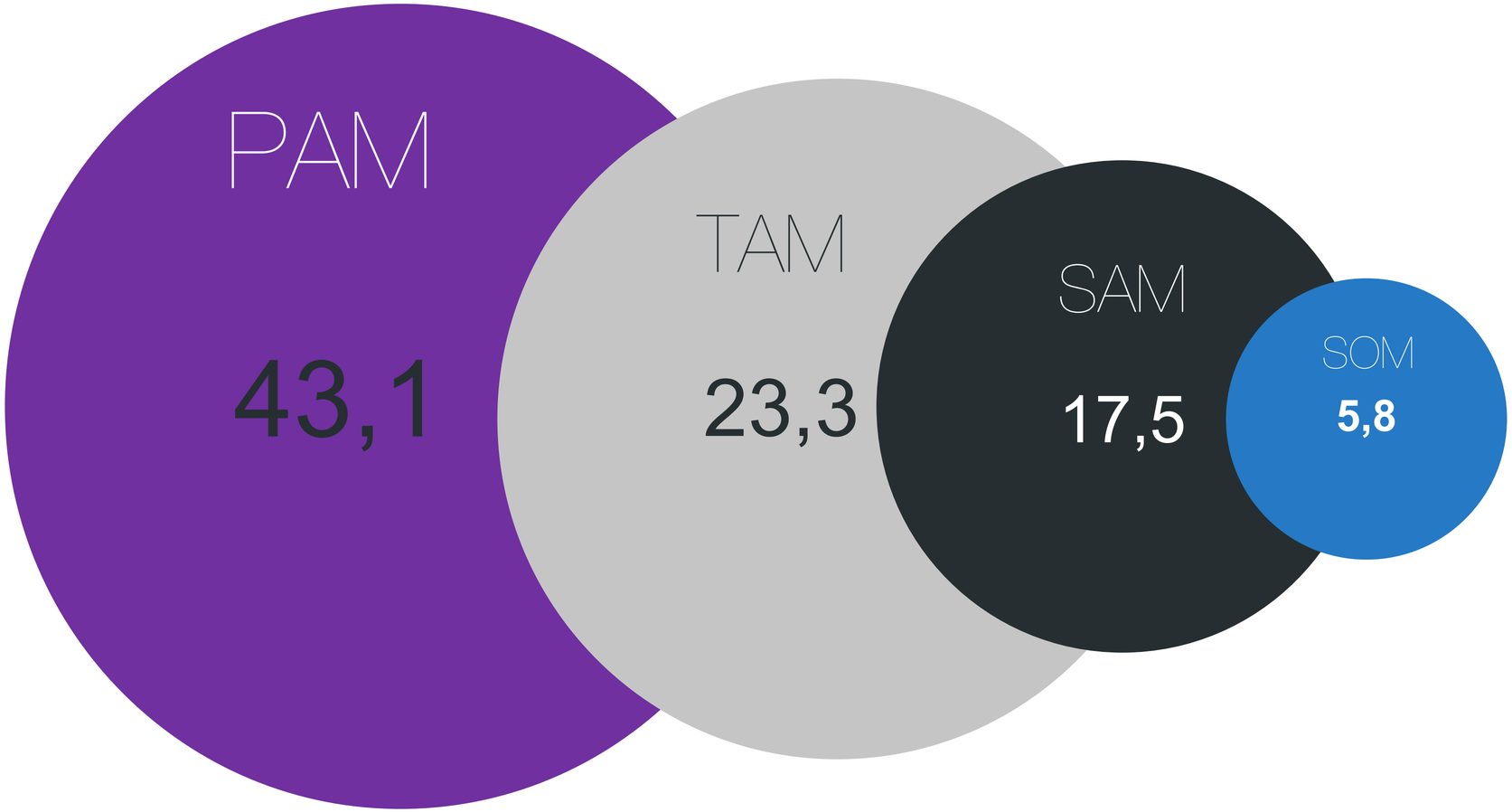


Сферы применения

Промышленные предприятия различных отраслей: телекоммуникации, электроэнергетическая отрасль промышленности, топливная промышленность, машиностроение и т. д.

Мировой рынок

В 2020 году общая стоимость продажи оборудования, программного обеспечения и сервисов, предназначенных для информационной безопасности (ИБ), достигла 43,1$ миллиарда, увеличившись на 5,6% относительно показателя годичной давности (40,8$ млрд). Такие данные 20 июля 2020 года обнародовали аналитики Canalys.



https://www.canalys.com/newsroom/canalys-global-cybersecurity-forecast-2020

Интеллектуальная собственность

Планируется запатентовать:

1.Алгоритм взаимодействия пользователя и информационной системы, который позволяет при необходимости выделить составляющую для конкретной отрасли в процессе оценки информационной безопасности;

2.Методику наполнения внутренней базы знаний экспертной системы;

3.Метод обнаружения вторжений на основе анализа среднеквадратической ошибки фильтрации трафика на заданном интервале времени для принятия решения о фиксации аномалий в сетевом трафике.

План реализации

№	Наименование работ	Примерные сроки (мес.)
1	Разработка модели базы знаний экспертной системы в области оценки информационной безопасности	3
2	Разработка (подготовка) теоретической основы базы знаний	3
3	Разработка алгоритма принятия решений	3
4	Исследование новых методов кибербезопасности в промышленных системах и цифровом производстве	3
5	Разработка алгоритма взаимодействия пользователя и системы	4
6	Разработка метода обнаружения вторжений на основе анализа среднеквадратической ошибки фильтрации трафика на заданном интервале времени для принятия решения о фиксации аномалий в сетевом трафике	6
7	Апробация и верификация	3
8	Разработка технологии комплексной оценки информационной безопасности промышленных систем и цифровых производств с учетом конкретной отрасли	1

Партнеры и потенциальные заинтересованные организации

Предприятия телекоммуникации, электроэнергетическая отрасль промышленности, топливная промышленность, машиностроение и т. д.

KASPERSKY lab

Check Point
SOFTWARE TECHNOLOGIES LTD

CISCO

Barracuda

paloalto NETWORKS®

ПГУТИ

«Разработка технологии комплексной оценки информационной безопасности промышленных систем и цифровых производств с учетом конкретной отрасли»

Филиппов Николай – руководитель проекта

8 937 984 888 3

kfilipppov@mail.ru