Реализация приоритетных задач информационной безопасности крупных организаций и госкорпораций и

оптимизация ресурсов в нынешних экономических условиях
(Заседание 10.02.2021 г.)

«Актуальные проблемы информационной безопасности в современных экономических условиях. Возможные решения и пути развития»

Докладчик: Заведующий кафедрой ИБ
доктор технических наук, доцент
Воробьев Евгений Германович

Кафедра «Информационная безопасность» Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина)

2021 г.

Четвертая промышленная революция

- Полная интеграция средств управления с объектами производства, энергетики, транспорта, медицины, обороны

Рынок интеллектуальных цифровых промышленных систем в России, млрд рублей

Источник: ГидМаркет

Прогноз динамики рынка микроконтроллеров для IOT и других применений в 2011–2019

(По данным корпорации ic insights)

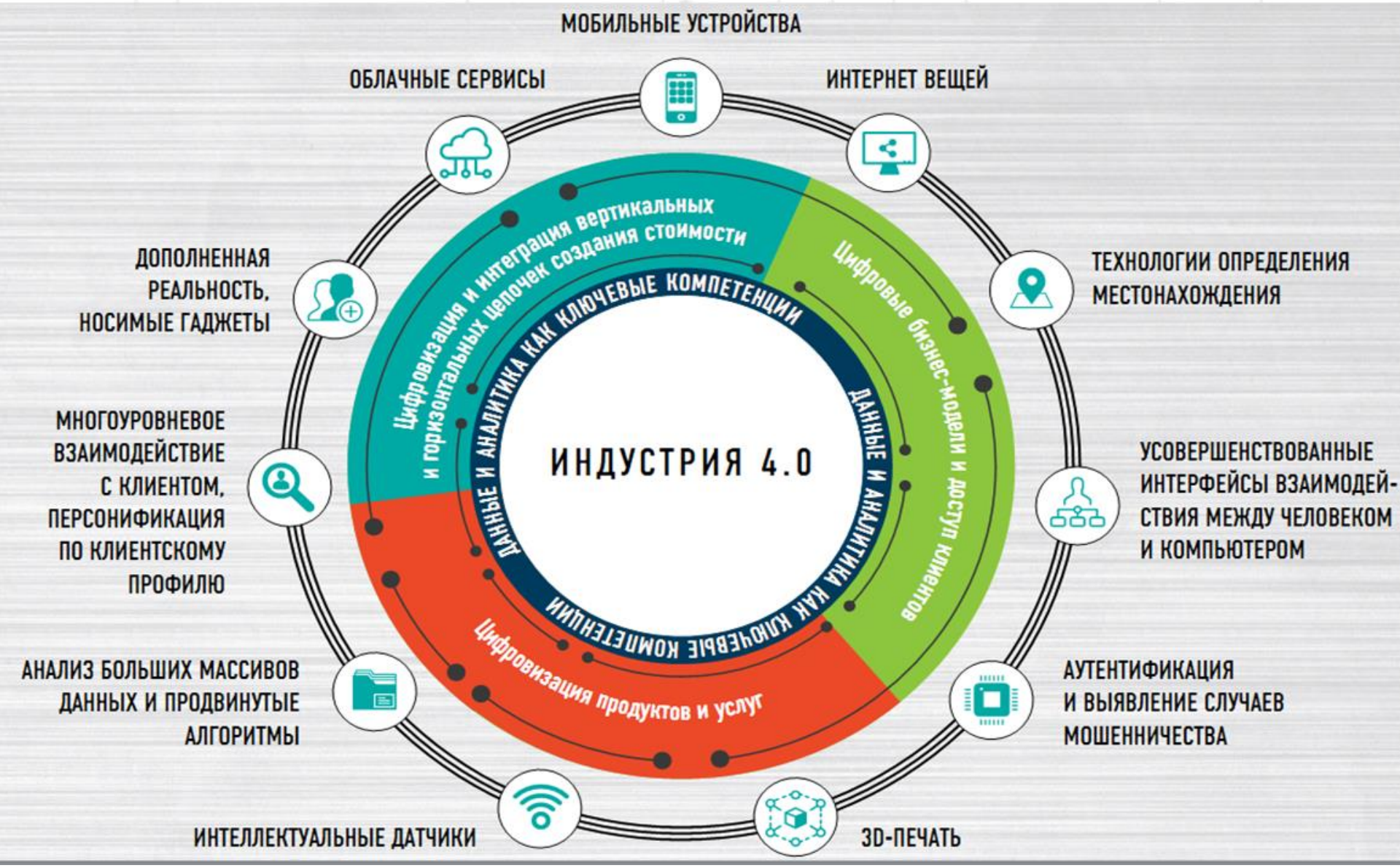
- В 2017 году произведено примерно 350 000 000 компьютеров

- В 2017 году произведено примерно 1 000 000 000 контроллеров
- По прогнозам в 2019 году может быть произведено до 2 000 000 000 контроллеров и до 2020 г. это количество будет расти

Прогноз динамики рынка микроконтроллеров для IoT и других применений в 2011-2021 гг.

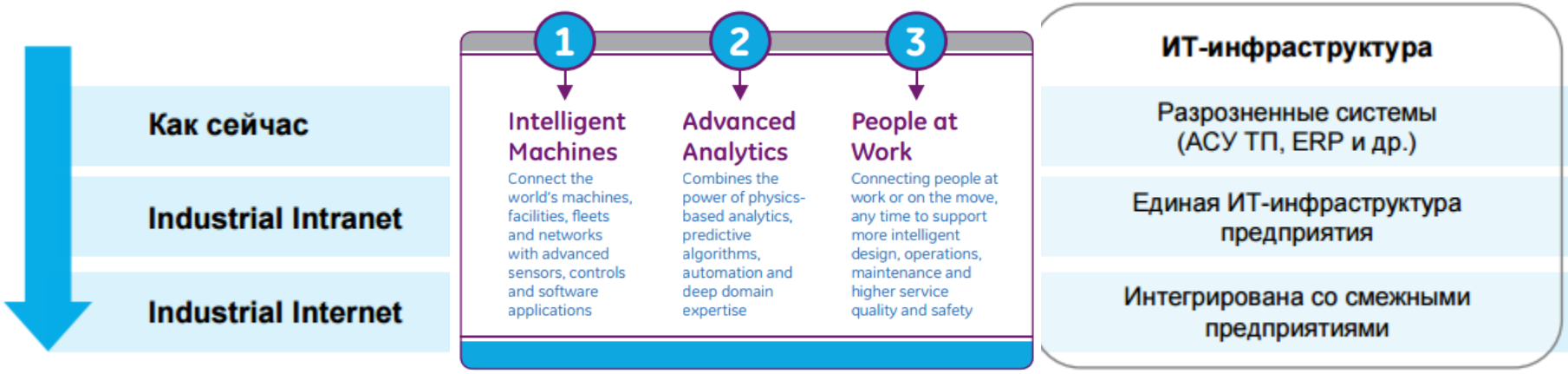
В 2020 - 21 г. произведено :
более 300 000 000 компьютеров;
примерно 2 500 000 000 контроллеров.

ЦИФРОВАЯ ЭКОНОМИКА



Интернет вещей (Internet of Things, IoT)

Интернет производственных систем (Industrial Internet)



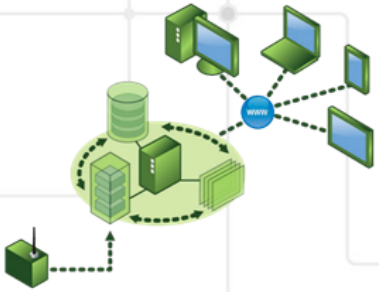
Киберфизические системы

Интеллектуальные роботы

– системы спутников,
– летательные станции

Системы беспилотных движущихся средств

– дроны,
– беспилотные автомобили,
– спутники



Scada-системы

– в энергетике,
– в медицине,
– в производстве,
– в обслуживании

Интернет вещей

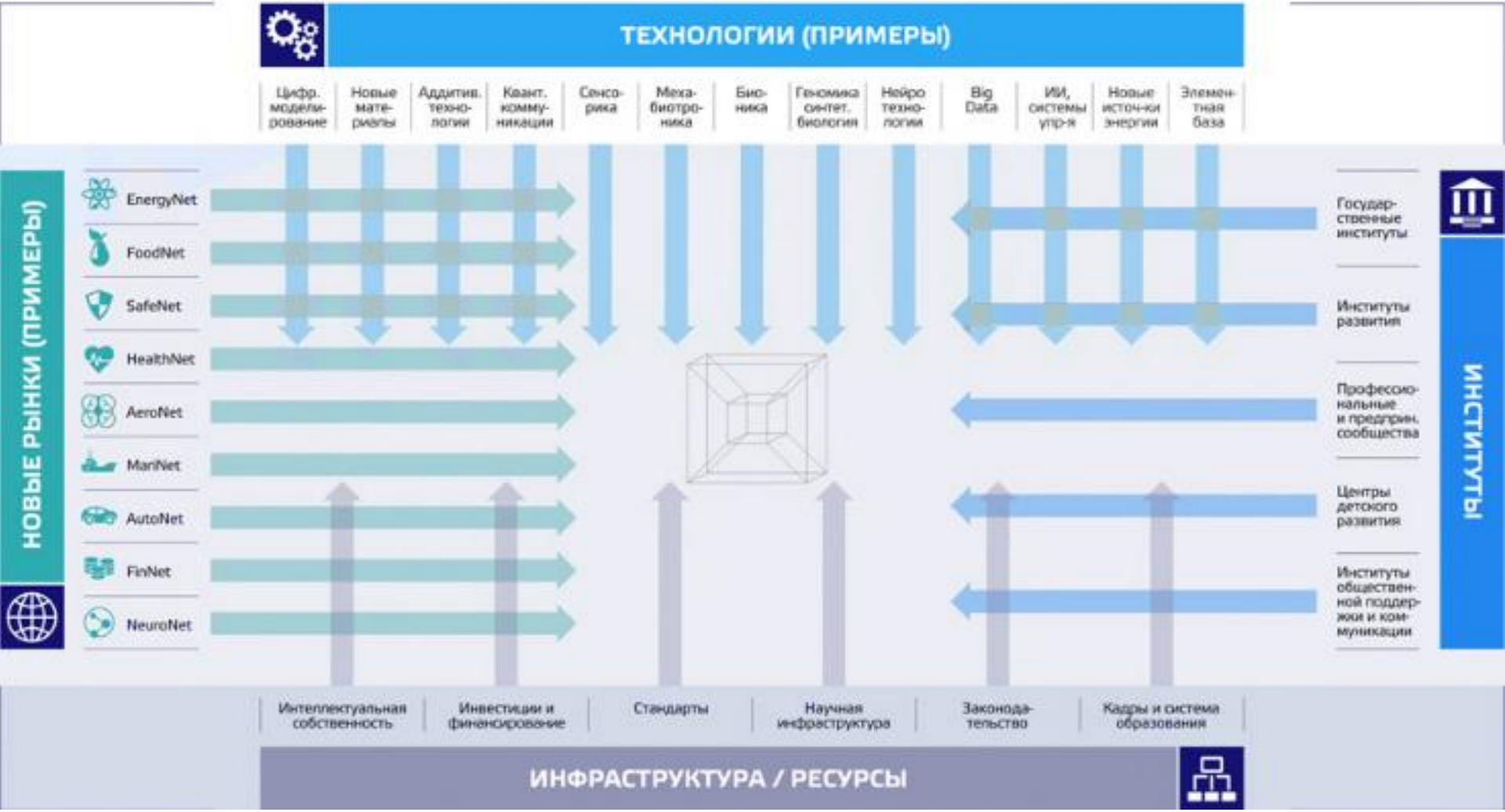
– встроенные системы,
– умный дом

Многоагентные системы

– промышленный интернет вещей,
– системы виртуализации,
– биоинспирированные системы,
– реконфигурируемые системы

Вовлеченность передовых ИТК-технологий в развитие цифровой экономики

Национальная технологическая инициатива РФ



Антропогенные угрозы

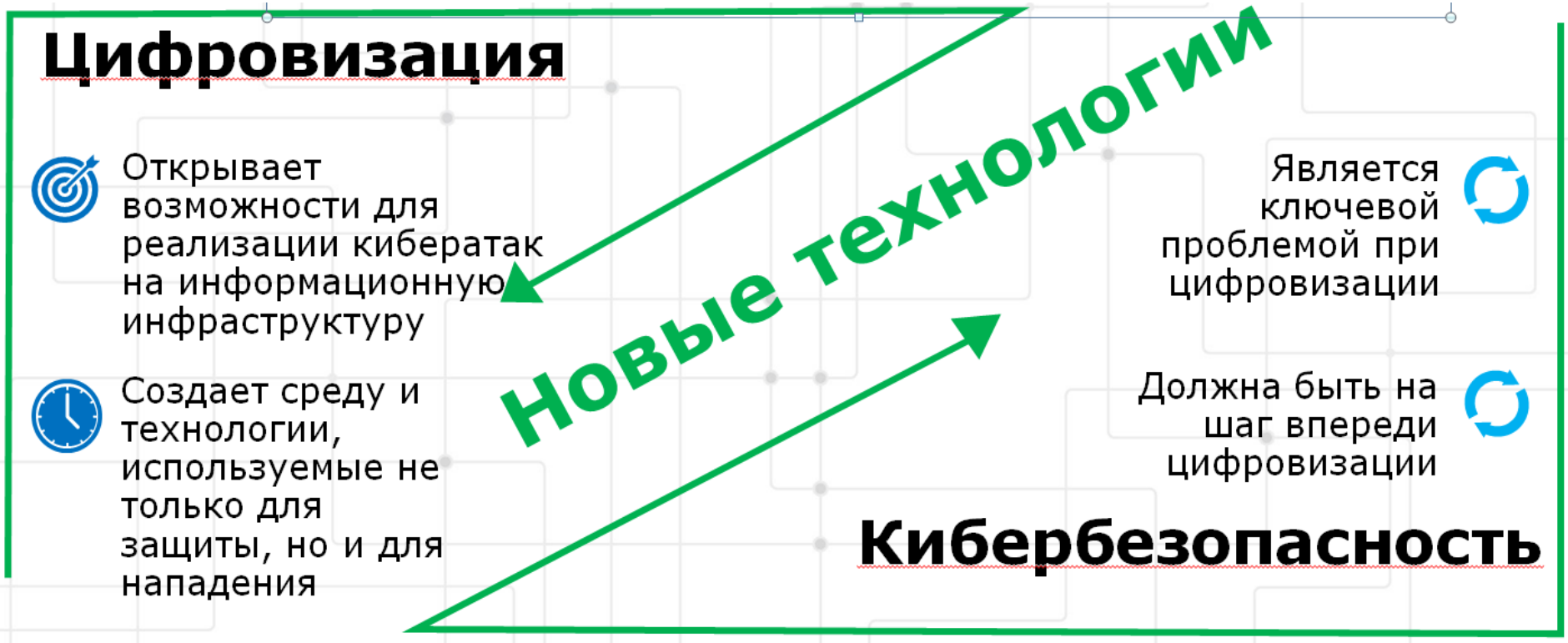
Существуют три общемировые группировки создающие угрозы безопасности и не скрывающие своих целей, живущие среди нас

1. «Глобальное информационное общество» .
   Позиция: Информация должна быть доступна каждому и без всяких ограничений

2. «Сторонники философии А.Азимова (3 закона робототехники)» .
   Позиция: Компьютерные системы опасны, нужно иметь встроенные каналы управления, а при необходимости и уничтожения

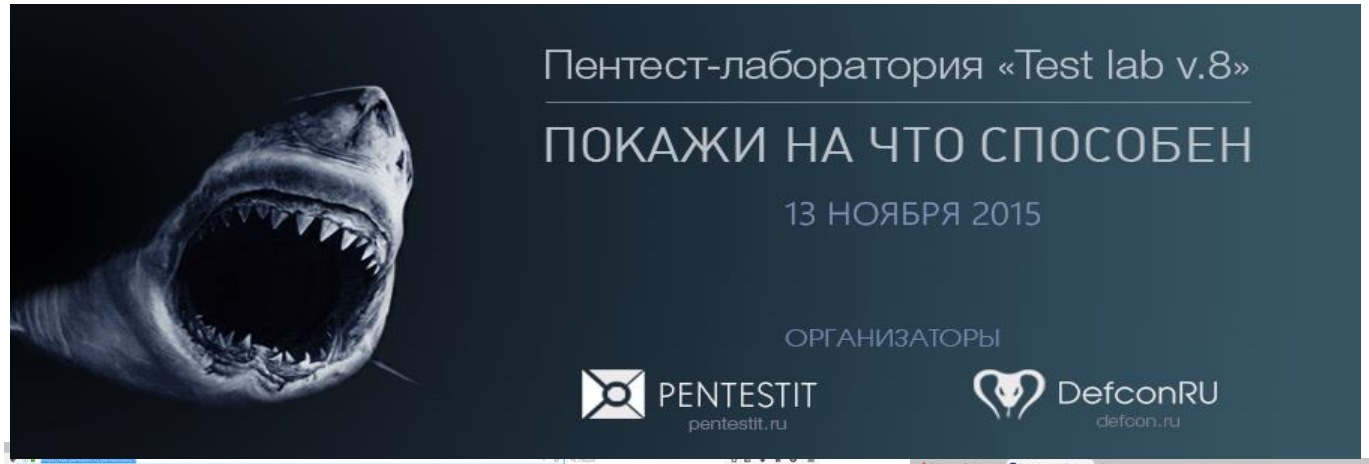
3. Хакерское сообщество.
   Позиция: Находят аппаратные и программные закладки созданные 1 и 2-й группой и используют их для личного обогащения

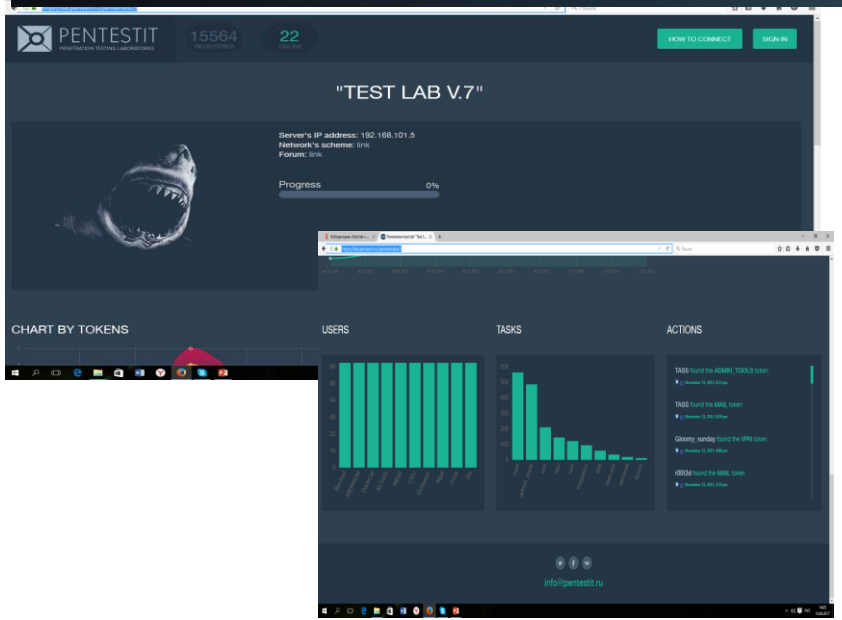
Цифровизация открывает широкие возможности для реализации угроз информационной и кибербезопасности

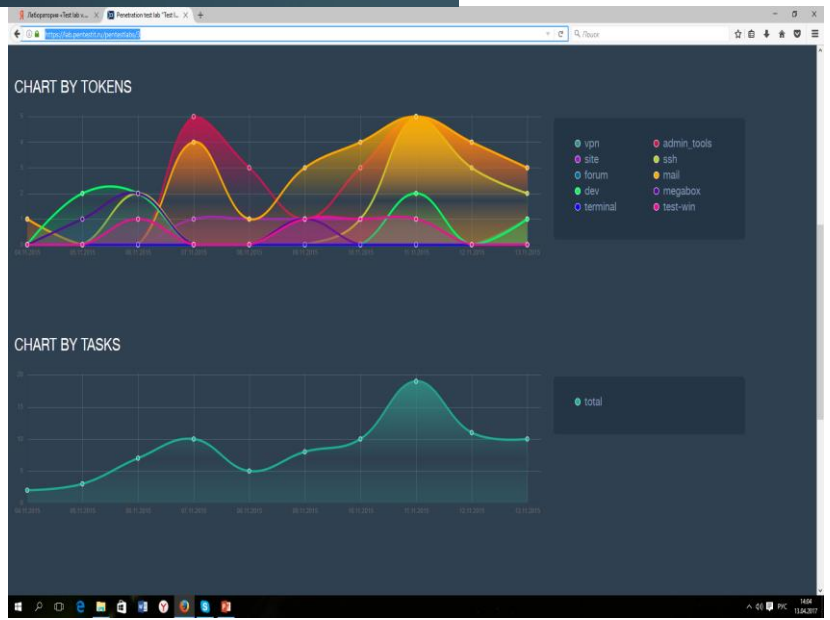


Тестирование на проникновение «этичный хакинг»

Лаборатории тестирования на проникновение «Test lab» имитируют ИТ структуру настоящих компаний и созданы для легальной проверки и закрепления навыков пентеста. Лаборатории всегда уникальны и содержат самые актуальные уязвимости.



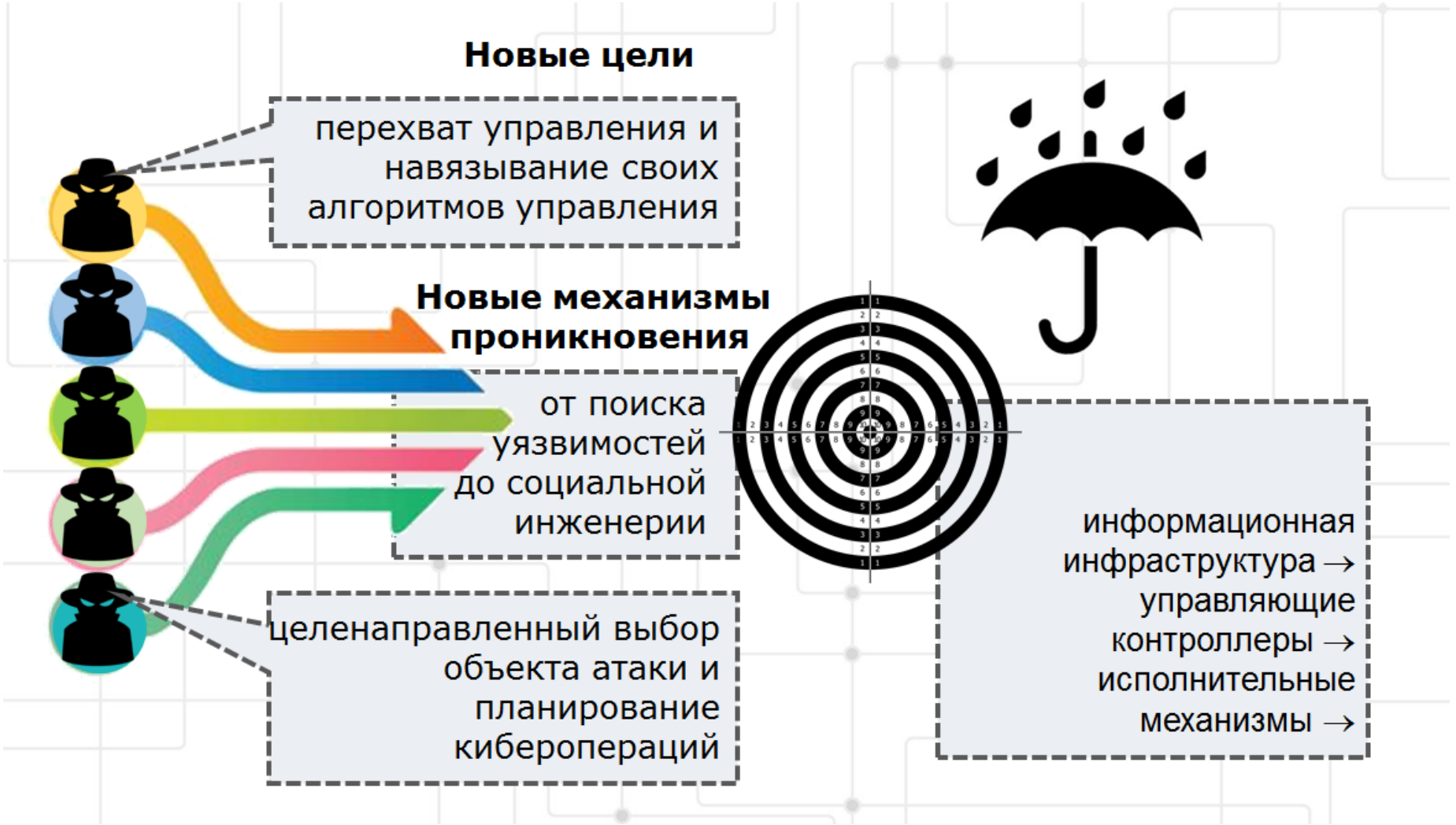




Проблема безопасности цифрового производства и цифровой экономики

- универсальность сетевых протоколов сети Интернет и принципов удаленного управления распределенными системами позволяет транзитивно замкнуть все управляющие системы производственной, финансовой и общественно-политической сферы в единое киберпространство
- глобальная доступность киберфизических объектов порождает проблему обеспечения устойчивой работы цифрового производства в условиях случайных и целенаправленных компьютерных атак, приводящих к долговременному и трудно обнаруживаемому воздействию на управление технологическими процессами, что может повлечь катастрофические последствия.

Отличия киберугроз от традиционных угроз ИБ



Требования новых нормативных документов ФСТЭК существенно увеличивают трудоемкость сертификационных исследований

1. Методика выявления уязвимостей и не декларированных возможностей утверждена ФСТЭК России 11 февраля 2019 г, применяется при проведении сертификационных испытаний с 1 мая 2019.
2. «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (Требования к уровням доверия)» утверждены приказом ФСТЭК России от 30 июля 2018 г. № 131, приказ зарегистрирован Минюстом России 14 ноября 2018 г. № 52686, вступил в силу с 1 августа 2018 г., применяется при проведении сертификационных испытаний с 1 мая 2019 г.

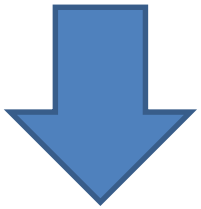
Новые вызовы - новые задачи кибербезопасности

Национальная технологическая инициатива (НТИ) — государственная программа мер по поддержке развития в России перспективных отраслей, которые в течение следующих 20 лет могут стать основой мировой экономики.

СейфНет - «кокон безопасности» для технических и компьютерных систем, которым мы не можем доверять

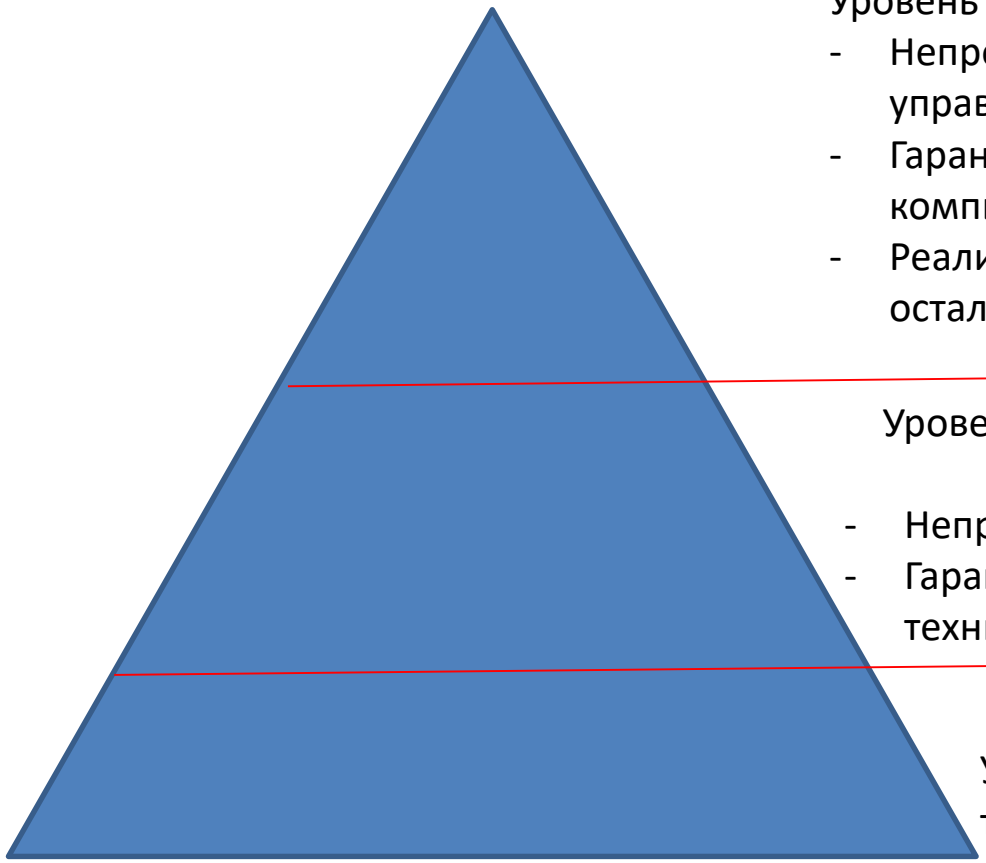
Концепция СейфНет

К 2025 году - барьер отчуждения между человеком и техногенной средой существования.
Человек не может нанести ущерба системе,
а система - человеку



К 2035 году – сращивание человека и системы
на основе нано и квантовых технологий.
Система умирает в случае смерти человека и наоборот.

Реализация концепции СейфНет



Уровень спецслужб (квантовые технологии)

- Непрослушиваемые каналы связи и управления
- Гарантированная защита от НСД в компьютерной технике
- Реализация «кокона безопасности» для остальных уровней

Уровень сетевых сервисов и технологий в рамках НТИ (импортозамещение)

- Непрослушиваемые каналы связи и управления
- Гарантированная защита от НСД в компьютерной технике

Уровень недоверенных компьютерных технологий

Практико-ориентированный подход к подготовке специалистов по ИБ

Цель данного подхода – приведение содержания и результативности образовательных программ в соответствие с современным уровнем технологической инфраструктуры и ожиданиями ведущих работодателей

Современный специалист по ИБ должен владеть методами решения следующих задач:

- Обнаружение и анализ киберугроз, направленных на нарушение киберустойчивости систем цифрового производства и цифровой экономики, робототехнических систем
- Реализация адаптивной активной системы предотвращения киберугроз с использованием методов искусственного интеллекта для управления параметрами и архитектурой защищенной системы
- Разработка методов безопасной обработки больших и сверхбольших массивов данных с использованием гомоморфной криптографии, создание глобальной доверенной среды с использование блокчейн и оптимизация информационных потоков на основе BigData.
- Разработка систем мониторинга, оценки состояния, расследования инцидентов кибербезопасности и киберустойчивости для прогнозного управления безопасностью цифрового пространства

Дополнения в УК РФ

Ответственность для тех кто «взламывает»

Деяние	Наказание
Создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на КИИ...	До 5 лет л/с штраф до 1 млн. руб.
Неправомерный доступ к охраняемой компьютерной информации, содержащейся в КИИ...	До 6 лет л/с штраф до 1 млн. руб.
Совершено группой лиц	До 8 лет л/с

Ответственность для тех кто обслуживает и защищает

Деяние	Наказание
Нарушение правил эксплуатации [ИТ] КИИ..., если оно повлекло причинение вреда КИИ	До 6 лет л/с
С тяжкими последствиями	До 10 лет л/с

Собственные образовательные сервисы и ведущих технологических компаний России в области информационной безопасности

«Яндекс»	Яндекс	• Академия Яндекса
Mail.ru Group (совместно с GeekBrains)	@mail.ru	• GeekUniversity
«Сбербанк»	СБЕРБАНК	• (АНО) «Корпоративный университет Сбербанка» • Академия кибербезопасности
Лаборатория Касперского	KASPERSKY lab	• Kaspersky Automated Security Awareness Platform (ASAP) – онлайн-платформа для организации тренингов по защите от киберугроз

Специалист должен владеть современными информационными технологиями

- Сетевые технологии: сети с переменной архитектурой, самоорганизующиеся сети, магистральные сети
- Облачные и туманные системы
- Эластичные и мягкие вычисления
- Суперкомпьютерные технологии
- Технологии искусственного интеллекта
- Современные базы данных
- Интегрированные мобильные системы
- Виртуальная и дополненная реальность

Общетеоретическая подготовка специалистов по ИБ должна базироваться на следующих областях знаний

- **Управление информационной безопасностью:** методы организации адаптивной динамической системы со стохастическими характеристиками, адаптивное управление с использованием искусственного интеллекта.
- **Криптографическая защита:** гомоморфная криптография, распределенные пост квантовые крипто алгоритмы, криптографическая защита в децентрализованных распределенных самоорганизующихся сетях, блокчейн.
- **Безопасность больших данных:** принципы работы с большими данными, защищенные системы интеллектуального сбора и предобработки неструктурированных данных, анализ данных в облачных системах и на гетерогенном вычислительном кластере, применение гомоморфной криптографии для обработки больших и сверхбольших массивов данных, методы динамического управления нагрузкой.
- **Киберустойчивость систем управления цифровым производством:** методы обеспечения глобального доверия и киберустойчивости, методы глубокого обучения для обнаружения уязвимостей в программном обеспечении, анализа вредоносных программ, распознавания сетевых атак, обнаружения бот-сетей и кибермошенничества.

ОСОБЕННОСТИ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО ИБ В СОВРЕМЕННЫХ УСЛОВИЯХ

Подготовку специалистов по ИБ в современных условиях отличают два связанных между собой фактора:

1. Конвергенция целей ИБ от противостояния угрозам к созданию систем, обеспечивающих сохранение полномасштабного функционирования информационных систем в условиях постоянно действующих компьютерных атак. Необходимость подробного изучения механизмов реализации угроз, уязвимостей, тестирования на проникновение и т.д.
2. Игровой характер противостояния средств защиты и угроз в киберпространстве, поддающийся моделированию с использованием технологий виртуализации и сетевых полигонов. Технологии виртуализации позволяют при относительно небольших затратах создавать адекватные макеты реальных систем и осуществлять моделирование киберпротивоборства.

Подготовка специалистов по актуальным направлениям деятельности в области ИБ

ПД ТР

ТЗИ

ОБ КИИ

Законодательство в сфере безопасности критической информационной инфраструктуры

- Федеральный закон от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
- Постановление Правительства РФ от 08 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»;
- Приказ Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. №235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;
- Приказ Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
- Приказ Федеральной службы по техническому и экспортному контролю от 22 декабря 2017 №236 «Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»;
- Приказ Федеральной службы по техническому и экспортному контролю от 6 декабря 2017 г. N 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации»;
- Постановление Правительства РФ от 17 февраля 2018 г. N 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
- Информационное сообщение Федеральной службы по техническому и экспортному контролю от 4 мая 2018 г. N 240/22/2339 «О методических документах по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры Российской Федерации».

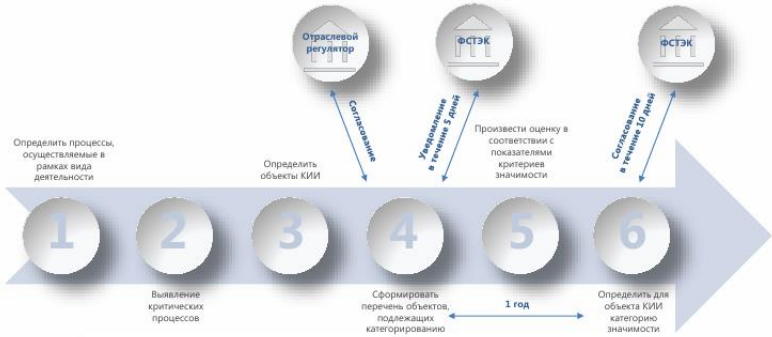
Перечень потенциальных сфер объектов КИИ

- здравоохранение;
- наука;
- транспорт;
- связь;
- энергетика;
- банковская и иные сферы финансового рынка;
- топливно-энергетический комплекс;
- атомная энергия;
- оборонная и ракетно-космическая промышленность;
- горнодобывающая, металлургическая и химическая промышленность.

Кто такой субъект КИИ?

Что означает «категорирование объектов КИИ»?

С кем осуществляется взаимодействие при категорировании объектов КИИ?



Система безопасности значимого объекта КИИ

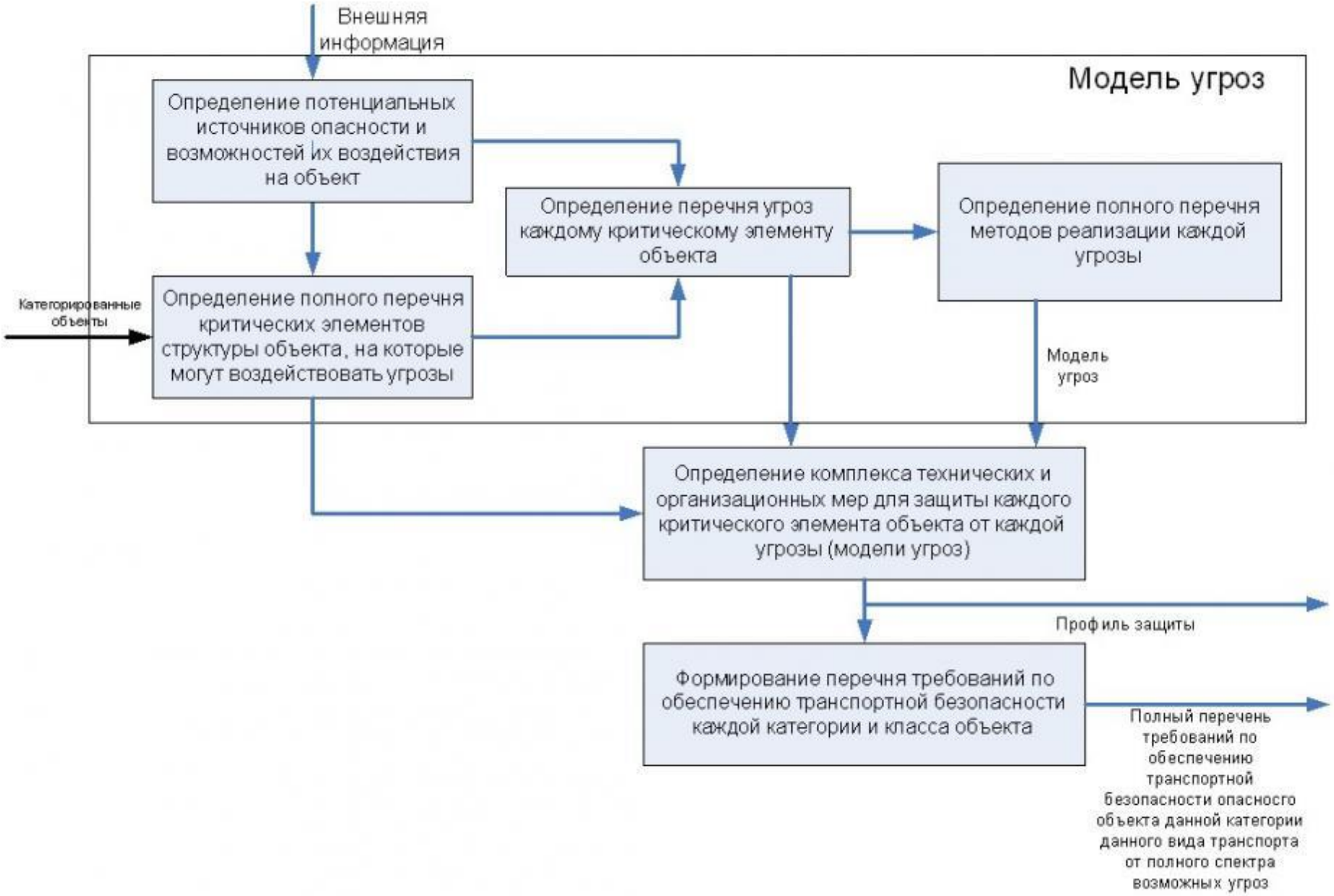
Реализация требований к ИБ включает в себя 5 базовых шагов:

Для значимых объектов КИИ, помимо интеграции в ГосСОПКА, субъекты КИИ должны:

✓Создать систему безопасности значимого объекта КИИ;

✓Реагировать на компьютерные инциденты. Порядок реагирования на компьютерные инциденты должен быть подготовлен ФСБ России до конца апреля текущего года;

✓Предоставлять на объект КИИ беспрепятственный доступ регуляторам и выполнять их предписания по результатам проверок. Законом предусматриваются как плановые, так и внеплановые проверки.


Внешняя информация
Модель угроз
Определение потенциальных источников опасности и возможностей их воздействия на объект
Определение перечня угроз каждому критическому элементу объекта
Определение полного перечня методов реализации каждой угрозы
Категорированные объекты
Определение полного перечня критических элементов структуры объекта, на которые могут воздействовать угрозы
Модель угроз
Определение комплекса технических и организационных мер для защиты каждого критического элемента объекта от каждой угрозы (модели угроз)
Профиль защиты
Формирование перечня требований по обеспечению транспортной безопасности каждой категории и класса объекта
Полный перечень требований по обеспечению транспортной безопасности опасного объекта данной категории данного вида транспорта от полного спектра возможных угроз

Национальный координационный центр по компьютерным инцидентам НКЦКИ

Согласно статьи 9 ФЗ-187 все без исключения субъекты КИИ обязаны информировать о компьютерных инцидентах федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Таким органом, в соответствии с приказом ФСБ №366 назначен НКЦКИ (Национальный координационный центр по компьютерным инцидентам).

Владельцам значимых объектов КИИ, в соответствии со статьей 10, вменена задача обеспечения непрерывного взаимодействия с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Помимо приказа о создании НКЦКИ, регистрацию в Минюсте прошли еще два приказа ФСБ №367 и 368, в которых утверждены перечни информации и порядок обмена информацией с ГосСОПКА.

Субъект может работать с ФСБ напрямую и направлять в НКЦКИ уведомления и запросы посредством почтовой, телефонной или факсимильной связи.

Уведомление – как направление уведомлений и запросов в рамках реагирования на инцидент между субъектами КИИ – допускается и по телефону, тогда как **информирование**, которое подразумевает, в числе прочего, и сообщение технических подробностей об инциденте – уже осуществляется с использованием технической инфраструктуры НКЦКИ.
В итоге – без подключения к ГосСОПКЕ субъектам КИИ не обойтись. А кроме того, еще необходимо помнить о соблюдении предписанных форматов обмена информацией с НКЦКИ.

Методы проведения аттестационных испытаний

Экспертно-документальный

Инструментальный

Проверка соответствия примененных параметров настройки элементов системы защиты информации требованиям безопасности информации

Проверка подсистем защиты информации от несанкционированного доступа

Проверка программной совместимости

Испытания системы защиты информации от несанкционированного доступа путем осуществления попыток несанкционированного доступа

ГОСТ РО 0043-003-2012, ГОСТ РО 0043-004-2013

ЗАДАЧИ НАЦИОНАЛЬНОЙ ПРОГРАММЫ «ЦИФРОВАЯ ЭКОНОМИКА»

К 2024 году…

… показатели направления «Кадры для ЦЭ»:

- 120 000 чел/год - выпускники образовательных организаций высшего образования по направлениям подготовки, связанным с ИТ
- 800 000 чел/год - количество выпускников ВПО/СПО, обладающих компетенциями в области ИТ на среднемировом уровне
- 40% - доля населения, обладающего цифровыми навыками

… показатели направления «Информационная безопасность»:

- 50% - доля граждан, повысивших грамотность в сфере ИБ, медиапотребления и использования Интернет-сервисов
- 97% - доля населения, использовавшего средства ЗИ от общей численности населения, использовавшего сеть Интернет в течение последних 12 месяцев

ЦЕНТР КОМПЕТЕНЦИЙ ЦЭ ПО НАПРАВЛЕНИЮ ИБ

18 декабря 2017 г.

УТВЕРЖДЕН
План мероприятий
по направлению «Информационная безопасность» Правительственной комиссией по использованию информационных технологий для улучшению качества жизни и условий ведения предпринимательской деятельности под председательством Председателя Правительства Российской Федерации
Д.А. Медведева

16 экспертных подгрупп:

- Устойчивость и безопасность функционирования единой сети электросвязи РФ (включая **российский сегмент Интернет**)
- Технологическая независимость и безопасность функционирования **аппаратных средств** и инфраструктуры обработки данных
- **Устойчивость и безопасность** функционирования информационных систем и технологий
- Правовой режим и технические инструменты функционирования сервисов и использования **данных**
- Правовой режим **межмашинного взаимодействия для киберфизических систем**
- Правовой режим функционирования машинных и когнитивных интерфейсов, включая **Интернет вещей**
- **Кадровое обеспечение** реализации направления ИБ

…

ПЛАН МЕРОПРИЯТИЙ И ПАСПОРТ ФЕДЕРАЛЬНОГО ПРОЕКТА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

- ✓ **2019 г.** : Формирование требований к созданию и внедрению **высокотехнологичных специализированных комплексов учебно-тренировочных средств** и **компьютерных полигонов** и иной материально-технической базе для организации образовательного процесса по программам в области информационной безопасности, разработка базовых лабораторных практикумов, направленных на формирование практических умений и компетенций в области обнаружения и противодействия компьютерным атакам, технологий и методов защиты информации

- ✓ **2021 г.** : Создание **испытательных полигонов** на базе российских ВУЗов по тестированию российских продуктов в области ИБ

- ✓ **2019-2021 гг.:** Введение в эксплуатацию **киберполигона для обучения и тренировки специалистов и экспертов разного профиля, руководителе в области ИБ** и ИТ \ современным практикам обеспечения безопасности.

КИБЕРПОЛИГОН

Киберполигон - инфраструктура для отработки практических навыков специалистов, экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий, а также для тестирования программного и аппаратного обеспечения путем моделирования компьютерных атак и отработки реакций на них

Типы:

- Информационно-технологический киберполигон – модель банковской автоматизированной системы
- Индустриальный киберполигон – АСУ ТП энергетического сектора

(Постановление Правительства РФ от 12.10.2019 №1320 «Об утверждении Правил предоставления субсидий из федерального бюджета на создание киберполигона …»)

ЛАБОРАТОРНАЯ БАЗА - КИБЕРПОЛИГОН

Киберполигон позволяет решать **задачи**:

- лабораторная база для передачи, отработки и закрепления навыков действия
- проведение фундаментальных, прикладных и поисково-экспериментальных исследований в областях защиты информации, кибербезопасности и киберустойчивости
- оценка эффективности систем с учетом требований их функциональности, стабильности и защищенности
- организация в режиме реального времени мониторинга состояния технического и иных видов обеспечения разрабатываемых либо существующих систем с возможностью принятия решений по устранению выявленных негативных ситуаций
- организация и обеспечение функционирования систем комплексной защиты на основе технических, программных, организационных и иных методов защиты для обеспечения требуемого уровня устойчивости и функциональности
- реализация методов и методик интеллектуальной поддержки принятия решений в условиях нечеткости и слабой структурированности
- обеспечение оптимизации, оперативного управления, мониторинга и контроля, прогнозирования и оценки предложенных решений при формировании управляющих воздействий в ходе функционирования защищенных систем и ПО

Спасибо за внимание!