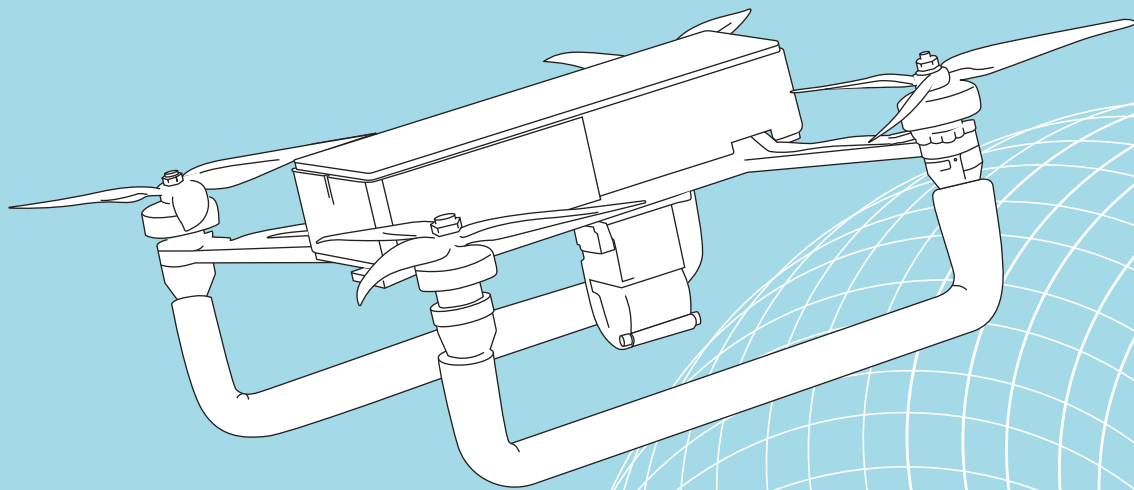


КИБЕР- ИММУНИТЕТ ЦИФРОВОГО НЕБА

По материалам панельной сессии
на форуме «Сильные идеи
для нового времени»



Москва, Национальный
центр «Россия»

Июль 2025

Об идее Кибериммунитета цифрового неба	4
Вступление модераторов	5
Доклады спикеров сессии «Новая эпоха освоения космоса и неба. Кибериммунитет цифрового неба»	6
Модели технологического суверенитета	16
Предложения	17



Кибериммунитет цифрового неба

Современные геополитические процессы, применение в авиационной и космической деятельности технологий двойного назначения, развитие и применение сквозных технологий формируют особый запрос на межотраслевое регулирование и необходимость появления документов, предусматривающих комплексный подход к различным видам безопасности при появлении и развитии видов экономической деятельности, связанных с применением беспилотных авиационных систем и освоением низкой околоземной орбиты.

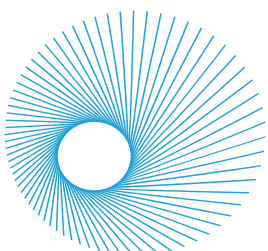
Развертывание «Цифрового неба» – безальтернативный сценарий построения новой архитектуры воздушно-космического пространства в первой половине 21 века под новые виды экономической деятельности с использованием беспилотных авиационных и малых космических систем.

Контроль над воздушным и околоземным космическим пространством является ключевым условием обеспечения суверенитета страны в 21 веке.

Кибериммунитет Цифрового неба определяется его стойкостью к существующим и будущим киберугрозам на протяжении всего жизненного цикла, который может составлять более 5 лет для наиболее критической информационной инфраструктуры.

Ключевые элементы:

- Конструктивная безопасность (Secure by Design)
- Доверенный искусственный интеллект
- Архитектура безопасности и доверия
- Отечественные криптографические методы
- Отечественные доверенные и защищенные аппаратные средства



**СИЛЬНЫЕ ИДЕИ
ДЛЯ НОВОГО
ВРЕМЕНИ**



Идея на крауд-платформе Форума
«Сильные идеи для нового времени»

смотреть видео



Андрей Силинг

Заместитель генерального директора
Агентства стратегических инициатив,
исполнительный директор
АНО «Платформа НТИ»



Самый большой вопрос, на который хочется найти ответ в ходе сегодняшней сессии, это как сделать так, чтобы идея «Кибериммунитета Цифрового неба» максимально быстро обрела плоть, овладела массами, получила необходимые ресурсы и масштаб реализации.

Предлагаю наш разговор построить вокруг ментального упражнения, связанного с мышлением.

- Мы говорим **в чем сила идеи**, в чем ее смысл и в чем ее польза.
- Далее мы думаем о том, **«почему эта идея провалится»**, в чем барьеры для ее реализации, почему это не получится. Мы называем эти барьеры, и думаем, как их преодолеть. Это барьеры в косности мышления, это барьеры в существующей модели интересов в отраслях и так далее. Самые разные барьеры: технологические, социальные, экономические.
- И наконец третьим тактом мы говорим, а **почему всё-таки это получится**, что мы сделаем для того, чтобы эта идея выстрелила и оказалась нашим ближайшим будущим.



Андрей Тихонов

Президент ассоциации «Доверенная
Платформа», со-руководитель рабочей
группы SafeNet НТИ



Идея «Кибериммунитета» принадлежит Евгению Касперскому, мы её начали активно развивать еще в 2021 году. Концепция Secure By Design, которую мы изначально замыслили, очень существенно расширилась и далее превратилась в дорожную карту Сейфнет.

Что такое кибериммунитет? Это подход к построению информационных систем, который подразумевает, что безопасность добавляется не как отдельный компонент, как это принято исторически, а закладывается на уровне архитектуры.

И при этом проектирование этих систем должно вестись с учетом рисков и безопасность должна быть интегрирована в каждом отдельном элементе. Концепция Цифрового неба предполагает создание единой цифровой платформы, которая будет объединять между собой беспилотные средства, спутники, платформы, наземные системы связи, мониторинга, контроля, конечные устройства.

Но развитие подобной системы связано не только с возможностями, но и с рисками. В данном случае эта инфраструктура может стать приоритетом для киберпреступников.

Нам нужно соблюсти максимальный технологический суверенитет, независимость в этом вопросе, при этом обеспечить максимальную безопасность, ну и в общем комфортные условия существования.



Александр Шойтов

Заместитель Министра цифрового развития, связи и массовых коммуникаций Российской Федерации



Основная дилемма – баланс между функциональностью и стоимостью с одной стороны и безопасностью и надёжностью, с другой стороны. SafeNet необходим, чтобы этот баланс соблюсти.

Нужны системы, в которые мы будем заранее закладывать этот подход на всём их жизненном цикле. Этот подход стратегически поддерживается государством.

Есть угрозы системные, а есть оперативные, которые сейчас возникают. То есть, если мы изначально всё правильно заложили и построили систему, это означает, что мы 90% угроз предотвратили уже на этом уровне.

Меры противодействия, мониторинг, реагирование – тоже уже заложены внутри системы. В этом случае мы сможем противодействовать угрозам.

Применяя концепцию Secure By Design, мы изначально строим систему так, что она может противодействовать различным видам угроз.

Однако есть и ряд сложностей с внедрением этих подходов.

- Это сложная технология, и, чтобы её внедрять, нужны высокие компетенции и затраты на этапе проектирования. После внедрения затраты будут минимизированы.
- Её сложнее реализовать если процесс уже построен. Интегрировать Secure By Design в действующую отрасль сложнее.
- Сложно применять, если используется много иностранных компонентов и технологий.
- Сложно применять, если отрасль тесно связана с другими.

С другой стороны, это гарантия информационной безопасности, в основе которой лежит криптография, позволяющая достигать гарантированной стойкости. У нас криптография своя, одна из лучших миров, свои стандарты с прошлого века, и все это признают. У нас практически все средства информационной безопасности есть. В этом случае мы выступаем в статусе лидера, и этим преимуществом надо пользоваться. За счет этого преимущества, подтягиваем все смежные отрасли.

Где наиболее эффективно применять Secure by Design?

- Там, где нужны гарантии.
- Там, где отрасль относительно изолированная. Цифровое небо – это как раз хороший пример.
- Там, где есть свои технологии и средства.
- Там, где относительно новая отрасль. Нет необходимости переделывать.

Цифровое небо – это та отрасль, в которой можно применить данную технологию и реализовать полный цикл конструктивной безопасности.



Кибербезопасность



Минцифры
России



Сергей Кукарев

Директор проектов по авиации
АО «ГЛОНАСС»



В рамках Концепции термин «небо» охватывает собой воздушное и околоземное космическое пространство. Определение «цифровое» указывает на то, что предметом Концепции является инфраструктура, элементы которой могут располагаться на земле, в воздушном или околоземном космическом пространстве, предназначенная для обеспечения информационного обмена широкого круга абонентов, в первую очередь, беспилотных воздушных судов.

Одним из ключевых элементов Концепции является доверенная среда перспективного цифрового воздушного и космического пространства как комплекс организационно-технических мероприятий для беспилотного транспорта.

Бизнесу и государству важно быстро пройти «нулевой уровень» и утвердить на уровне основ государственной политики и предварительных национальных стандартов правила «игры» для производителей беспилотного транспорта в области будущей информационной защищенности.

Геостационарная орбита
Средние орбиты
Низкие орбиты
Стратосферный уровень
Логистический уровень
Хозяйственный уровень
Транспортный уровень
Инфраструктурный уровень

ЦИФРОВОЕ НЕБО



Дроносфера как сетевая киберфизическая система

- единая архитектура цифрового неба с протоколами доверия
- подлежит правовому регулированию
- соблюдает иерархию отношений между элементами системы
- включает подвижные автономные объекты
- имеет обеспечивающую инфраструктуру
- самоорганизуется

Цифровое небо:

- объединяет уровни воздушного и космического пространства в архитектуру, требующую сквозного регулирования
- насыщается элементами критической информационной инфраструктуры (дроны и спутники), интегрированными в коммерческие сервисы, подключенные к гибридным сетям связи



Бесшовное
цифровое небо



АО ГЛОНАСС



Андрей Духвалов

Стратегический архитектор Лаборатории
Касперского



Цифровое небо рассматривается как
сложнейший информационный продукт.

Мы знаем, что информационные
продукты подвергаются атакам. Как
предполагается строить стратегию
устойчивости, безопасности и доверия
системы?

Очень простой ответ – Кибериммунитет.
Но на техническом языке мы привыкли
называть это конструктивной
информационной безопасностью
или Secure by Design.

В его основе лежат несколько простых
принципов, придерживаясь которых
можно строить информационные
системы таким образом, чтобы они
были устойчивы и выполняли свою
основную функцию даже в условиях
информационной и агрессивной
информационной среды.

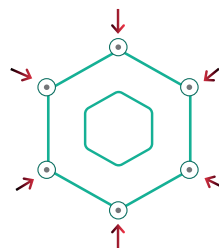


Кибериммунный
подход к разработке

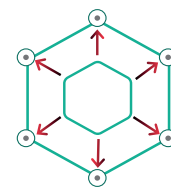
kaspersky

Принципы Кибериммунитета

- 1. Безопасность информационной системы не может быть лучше, чем задание к ней.** Этот простой тезис говорит о том, что информационная безопасность любой системы начинается с того, как мы ее представляем в начале разработки задач. Технические требования, с точки зрения методики, должны содержать не только требования бизнес-характера, но и требования по информационной безопасности. Если они закладываются в начале разработки системы, то система будет учитывать эти особенности и будет безопасна по факту своей разработки.
- 2. Изоляция.** Надежное разделение информационной системы на домены и наделение их атрибутами безопасности в рамках ассоциированной политики безопасности позволяет локализовать любые нарушения политики как в доверенных, так и в не доверенных компонентах
- 3. Наблюдаемость взаимодействия между системами.** Основные критические компоненты, отвечающие за безопасность, должны понимать, что происходит с системой, как компоненты обмениваются информацией и соотносить это с требованиями безопасности, которые наложены на систему и могут меняться в зависимости от того, какие новые угрозы возникают. То есть для разработанной ранее системы будет действовать политика безопасности, соответствующая новым угрозам.



ЗАЩИТА



ИММУНИТЕТ

Совокупность этих принципов позволяют достичь того волшебного состояния, когда мы можем делать доверенную систему из совокупности доверенных и недоверенных компонентов.

Вот такие основные подходы, если распространить их на цифровое небо, о котором мы сейчас рассказываем, позволяют сделать эту сложнейшую информационную систему таким образом, что мы сможем ей доверять на протяжении длительного времени.



Арутюн Аветисян

Директор Института
системного программирования
им. В.П. Иванникова РАН,
академик РАН



Безопасность — это значительно более широкое и сложное понятие, чем мы иногда думаем. Идёт массовое внедрение технологий, они постоянно развиваются как живой организм, а значит и инструменты обеспечения безопасности должны развиваться.

У нас есть много хороших компаний, которые работают в этой области. «Лаборатория Касперского» — это лидер, но есть и другие небольшие компании, которые тоже разрабатывают достойные продукты мирового уровня.

Я горжусь, что и наш институт делает свой вклад: мы заместили лучшие мировые аналоги и сегодня более двухсот компаний используют наши технологии безопасной разработки.

Почему «Цифровое небо» и «Кибериммунитет»?

Во-первых, очевидно, что ни в какой области, не только в Цифровом небе, без обеспечения нужного уровня безопасности невозможно внедрение технологий. В области искусственного интеллекта это положение зафиксировано в нашем стратегическом документе, подписанном в феврале 2024 года Владимиром Путиным («Стратегия научно-технологического развития Российской Федерации»). В нем четко прописано, что в критических областях и госуправлении необходимо внедрять доверенные технологии.

Цифровое небо — это очень наукоёмкая область с большим числом участников, имеющая много уровней, включая космос и низкие орбиты. Беспилотные аппараты внедряются в сельском хозяйстве, логистике и не только. И если эту наукоёмкую область мы с самого начала будем развивать фрагментарно, базируясь на сугубо рыночных механизмах, без глубокого вовлечения науки и государства, то мы не сможем быть конкурентоспособными и всё, что мы сделаем, будет не просто в разы, а в десятки раз дороже. Я не против рыночных механизмов, но в данном случае их недостаточно; в создании Цифрового неба мы должны объединить усилия.

Средства разработки должны создаваться открытыми сообществами внутри страны, чтобы мы все вместе контролировали ситуацию, а не каждый участник рынка, кто разрабатывает своё «железо», вынужден был бы поддерживать полностью весь стек системного ПО. Это невозможно. Всех существующих специалистов с учётом тех, кого сейчас готовят университеты, не хватит. Подковать блоху можно, нет проблем, мы создадим любую систему, но важно сделать систему, которая долгосрочно, как хорошее вино, с каждым годом становится лучше и устойчиво развивается. И это особенно важно, когда мы говорим о такой сфере, как Цифровое небо, которое будет с каждым годом всё более актуально и более востребовано.



Сборник технологий
ИСП РАН



Telegram-канал
ИСП РАН

ИСП **РАН**



Дмитрий Башкатов

Директор дивизиона гражданских технологий Агентства стратегических инициатив



Мы сейчас находимся в переходном периоде, когда нам нужно прекратить делить технологии на «гражданские» и «военные», любая технология становится «гражданско-военной».

Что мы видим? Любую гражданскую технологию можно использовать для решения не самых мирных задач. К сожалению, любую.

Поэтому «гражданских» технологий, которые не «военные», в мире с каждым днем будет все меньше и меньше. Найдут применение.

Вспоминаем случай, который сделали израильские спецслужбы с пейджерами.

1. **«Гражданско-военная интеграция»** это про правильное отношение к тому, что мы делаем, про технологии, как нам с ними жить и как нам с ними работать.

Это вызов с точки зрения проектирования, применения и понимания, что произойдет в завтрашнем дне.

2. **Второй вызов, который у нас есть — это искусственный интеллект.** Собственно, именно он в том числе может сделать любую самую мирную технологию с непредсказуемым опасным применением, разработав и просмотрев миллионы вариантов.

У нас две существенные особенности искусственного интеллекта: первое — это непрозрачность решений. Вспоминаем фантастику, в чём смысл жизни — ответ 42.

Почему 42? Непонятно. Мы не сможем понять, почему искусственный интеллект пришёл к такому ответу. Он производит значительно больше вычислений в секунду чем мы.

И второй момент. Небольшое изменение на входе задачи с использованием искусственного интеллекта может привести к непредсказуемым изменениям на выходе.

3. **Третий вызов, который мы получаем с наступлением «Эры автономной авиации».** С точки зрения нашей с вами повседневной жизни, всё большим количеством событий будут управлять алгоритмы искусственного интеллекта. Возвращаясь к двум моим предыдущим тезисам — мы не будем понимать процесс. Нам надо этому доверять, но доверять этому невозможно.

Если мы не можем прогнозировать результат, не видим прозрачности и не можем проверить, у нас нет той же вычислительной мощности, мы по умолчанию не будем доверять. Поэтому очень важен тезис Андрея Тихонова, про доверенную среду. В среду из доверенных элементов я не верю совсем, а вот доверенная среда из недоверенных элементов, как цель мне кажется ближе.

И последнее, почему всё-таки мы здесь сейчас заостряемся на небе, хотя сквозным образом это всё справедливо для всей нашей жизни. Небо граничит со всем.

И последнее, мы с вами все привыкли, что кибербезопасность это про базы данных, информационные системы государства.

Как только мы с вами говорим о небе, в нем летают конкретные устройства, мы начинаем физически чувствовать угрозу, поэтому для нас, для общества, «Кибериммунитет Цифрового Неба» не просто важен, он в кратчайшие сроки необходим для исполнения.



АГЕНТСТВО
СТРАТЕГИЧЕСКИХ
ИНИЦИАТИВ



Андрей Потёмкин

Заместитель главы
Росавиации



Цифровое небо – это неизбежность.

Международное регулирование гражданской авиации осуществляется на площадке ИКАО (подразделение ООН). Еще в прошлом десятилетии ИКАО приняло Стратегию, где одним из ключевых тезисов заявлено следующее: «Все, что может быть соединено, должно быть соединено». Имеются в виду радиоканалы связи и цифровой обмен данными.

В развитие этой Стратегии Глобальный аэронавигационный план ИКАО предусматривает в обозримой перспективе переход к использованию для задач авиации, включая аэронавигацию, общедоступных сетей связи.

В первую очередь, подразумевается использование технологий LTE и перспективных спутниковых технологий связи.

У концепции цифрового неба должны быть заказчики.

В Концепции сделан акцент на беспилотных транспортных средствах, в частности на авиационных. Действительно, беспилотным воздушным судам нужна связь, в особенности для контроля и управления. Сегодня нормативно установлено обязательство по обеспечению ее непрерывности. В этой части необходимо обеспечить технологический суверенитет.

В качестве примера можно привести опыт большой авиации.

В 2022 году из России ушли компании SITA и ARINC, которые обеспечивали цифровую радиосвязь между центрами управления полетами авиакомпаний, пилотами и диспетчерами.

Пришлось вернуться от цифрового к голосовому обмену, а также отказаться от дополнительных функций, повышающих эффективность совместной работы.

Это урок, который мы выучили и нам удалось избежать последствий. Например, не пришлось снижать интенсивность полетов, ограничивать пропускную способность аэродромов и воздушного пространства, так как голосовой обмен все еще позволяет работать эффективно. Но в перспективе «откатиться» на традиционные технологии в подобных случаях будет все сложнее, поэтому чтобы исключить вероятность сокращения перевозок и авиационных работ необходимо обеспечить не только цифровое небо, но и его независимость и кибериммунитет.

Авиация точно должна быть заказчиком концепции цифрового неба, но не единственным. Достаточно привести в пример ГЛОНАСС, Иридиум, Старлинк и многие другие проекты. Там много заказчиков, есть «якорные».

В этой концепции тоже нужно определить «якорных» заказчиков. И на наш взгляд, дроны – не самый сильный сегодня заказчик. Но в среднесрочной перспективе могут им стать.

Стандарты – от универсальных к специализированным

Для примера можно провести аналогию с семейством стандартов 3GPP, где сегодня уже прописаны дроны. Но перед тем, как появились стандарты по дронам, появилась сеть связи и стек технологий, уверенно развивающихся. Дроны там – один из потребителей, и специализированные стандарты появились позже, чем общие унифицированные.

Например, с точки зрения прикладной задачи контроля и управления беспилотником, мы сегодня ориентируемся

на логическую архитектуру «внешний пилот – беспилотник» или «система – беспилотник» со своими стандартами по обеспечению целостности, достоверности и непрерывности в зависимости от условий выполнения полетов. Мы рассчитываем, что на прикладном уровне будут применимы как сети наземной подвижной связи, так и спутники. Появление псевдоспутников, как элемента общей архитектуры, поможет развитию беспилотной авиации, в особенности в тех задачах, где требуется работа с полезной нагрузкой в режиме «онлайн».





Вячеслав Тёмкин

Основатель
ООО «ЭКИПО»



При обсуждении Цифрового неба важно представить перспективные технологические решения, которые будут его населять.

В низком космосе становится тесно, растут группировки спутников, появляются новые игроки, увеличивается количество космического мусора.

Основной недостаток использования этих высот заключается в наличии остаточной атмосферы, которая тормозит движущийся спутник, и без постоянно работающего двигателя коррекции орбиты он быстро сойдет с орбиты, мы его «потеряем». Современные двигатели коррекции проблему длительного удержания спутников на высотах 150–200 километров не решают. В условиях постоянного торможения двигателям коррекции необходимо непрерывно работать, и они быстро израсходуют взятый с Земли запас топлива, после чего спутники также сойдут с орбиты.

С другой стороны, данный недостаток одновременно является преимуществом. На этих высотах находится такой баланс газов остаточной атмосферы и сопротивления, которое она создает, при котором мы можем эффективно извлечь энергию из этих газов остаточной атмосферы, достаточную для парирования этого сопротивления (торможения). На этом была построена концепция нашего проекта – атмосферного ионного двигателя, который позволит длительно удерживать спутники на высотах 150–200 км.

Многие ученые занимаются созданием атмосферного ионного двигателя. Большинство из них идут по пути создания механических воздухозаборных устройств для атмосферного ионного двигателя, которые должны обеспечить достаточный уровень ионизации газов остаточной атмосферы. Но, к сожалению, они ничего действенного пока показать не могут.

Мы пошли другим путем и исключили из конструкции двигателя механические воздухозаборные устройства. Для ионизации газов остаточной атмосферы мы применили нестационарные открытые электромагнитные ловушки. Это совокупность электромагнитных катушек определенной конструкции, которые создают особую конфигурацию электромагнитных полей, обеспечивающих эффективную ионизацию.

Но в низком космосе есть диапазон высот 150–200 километров, который может быть эффективно использован для решения различных задач.

Эти высоты находятся ближе к Земле, что позволяет решать задачи более эффективно, и, в настоящее время, они никем не заняты.

Что позволяет нам зажигать и удерживать плазму в вакууме, соответствующем высотам до 220 километров. Мы добились извлечения тяги и ведем работу по ее улучшению.

Кроме того, мы приступили к созданию спутника-низколета, оснащенного атмосферным ионным двигателем. Это непростая задача, она усложняется тем, что, разработку проводим за счет собственных средств. Тем не менее мы движемся вперед и начали работу по созданию российской системы лазерной спутниковой связи.

В любом случае рано или поздно эти высоты будут кем-то заняты, и вот здесь можно поразмышлять, к чему это приведет. Безусловно – это управление беспилотной техникой из низкого космоса. Управления не только беспилотными летательными аппаратами, но и беспилотными автомобильным транспортом и беспилотными надводными средствами, которые в недалеком будущем станут обыденными. Эффективнее решения не придумаешь. Конечно же появятся прорывные решения в области связи, без использования наземной инфраструктуры – «спутник-смартфон-спутник». Из нижнего космоса будут эффективно контролировать изменения в лесных массивах, выполнять паспортизацию сельскохозяйственных земель, паспортизацию полос отвода земельных участков под различные объекты и многое другое. В принципе, для таких решений в России уже сейчас практически всё есть. Осталось покорить низкий космос.

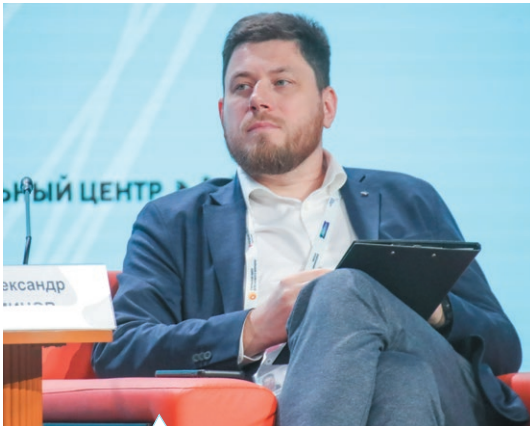
Мы благодарны коллективам АСИ и НТИ за оказываемую поддержку и надеемся на ее продолжение.

Действительно, уровень развития техники позволяет рассматривать «ближний космос» в качестве бесшовной системы с земной и воздушной средой. Осознание такого подхода и правильная реакция позволят нам опередить «западных соседей» и сформировать собственный передовой путь достижения технологического суверенитета.



Идея «Превосходство
в низком космосе»





Александр Минов

Генеральный директор
ООО «МТ-Лаб»



Для включения проектов «бесшовного неба» в экономический оборот необходимо преодоление административных барьеров и внедрение доверенных информационных систем.

Например, сейчас контрольные просмотры снимков дистанционного зондирования Земли, снятых дронами, занимают 30 дней. А хочется – получать к ним доступ в режиме онлайн. И это возможно уже сейчас с использованием тех самых информационных систем геопространственной осведомленности, которые в том числе наша компания развивает.

Важно преодолевать административные барьеры и совместно расширять применение доверенных платформ.

Необходимо регулирование дистанционного зондирования Земли из космоса и с дронов. Например, мы будем работать над тем, чтобы дроны могли летать по подстилающей поверхности на базе цифровых моделей местности. И это надо как-то регулировать. Эти модели надо актуализировать, эти модели должны быть доверенными, чтобы дрон не только вместо пиццы не принёс что-нибудь не то, но и не влетел куда-нибудь не туда.

Чтобы концепция «Цифрового Киберимунного Неба» была реализована, необходимо объединение регулятора, профильных ассоциаций, таких как «Доверенная платформа», НТИ, АСИ, бизнеса, с целью ликвидации административных барьеров. И наоборот, в некоторых случаях целесообразно дополнительно регулировать новое применение бесшовного цифрового неба с учётом всех вопросов безопасности, потому что, как сказал Арутюн Ишханович Аветисян, безопасность – это чуть шире, чем кибербезопасность.





Александр Селютин

Председатель совета директоров
ГК «Техноджет»



Понимая все проблемы, которые возникают в области кибербезопасности передачи данных, мы более 10 лет назад составили в инициативном порядке для себя техническое задание и начали разрабатывать совершенно новую систему передачи данных, включающие наземный и спутниковый сегмент.

Спутниковый сегмент обеспечивает гарантированную связь всем абонентам системы в любой точки Земли. Нами был создан собственный российский транспортный протокол, который работает на уровне L4, была создана система идентификации и маршрутизации всех абонентов.

Данный протокол включает в себя поддержку изменения доплеровских частот, что обеспечивает стабильной связью любых абонентов, которые внутри атмосферы передвигаются на доступных современным подвижным транспортным средствам скоростях.

Структура транспортного протокола не известна нашим зарубежным конкурентам, при этом он прекрасно работает на существующем сегодня сетевом оборудовании. Наличие такого решения является одним из основных элементов критической инфраструктуры.

В рамках спутниковой системы мы также начали писать собственную операционную систему. Стадия ее готовности 93%. На сегодняшний день мы прошли множество различных испытаний, включая совместные испытания с госкорпорацией Роскосмос. Проект имеет очень большую перспективу и интегрируется с цифровым небом.

Мы всегда открыты и готовы к взаимодействию с теми, кто хочет присоединиться к развитию данной системы.



Итоговые тезисы

СИЛИНГ АНДРЕЙ
ЛЕОНАРДОВИЧ



“

Нам нужна модель долгосрочного развития, которая позволяет в десятки раз, на порядки, увеличивать эффективность использования человеческого капитала, потому что и компетенции у нас есть, и решения у нас есть, но нам не хватает скорости, нам не хватает концентрации.

В этом году в период с 7 по 17 августа в Сколтехе пройдёт проектно-образовательный интенсив «Архипелаг 2025».

Мы будем говорить о будущем цифрового неба, о будущем кибербезопасности, о будущем самых разных ещё технологических областей, которых мы сегодня здесь касались.

И главное, что этот Архипелаг, будет впервые международным.

ТИХОНОВ АНДРЕЙ
ИВАНОВИЧ



“

При работе над SafeNet, мы увидели, что задача существует примерно в семи технологических переделах.

От электронной компонентной базы до интеграции и работы с требованиями.

И на каждом из этих этапов применима концепция конструктивной безопасности. Всем участникам необходимо договориться и для этого нужны, в первую очередь, нормативные механизмы.

НТИ может стать площадкой для тщательной работы над системой стандартов, которые объединяют и сшивают эту огромную конструкцию между собой.

Панельная сессия «Новая эпоха освоения космоса и неба. Кибериммунитет Цифрового Неба» форума «Сильные идеи для нового времени» 2025



смотреть
видео

Модели технологического суверенитета

Технологический суверенитет

Способность страны разрабатывать и применять критически важные технологии, чтобы оставаться независимой и конкурентоспособной. Эти технологии позволяют организовать производство товаров в ключевых сферах деятельности общества и государства.



ts.nti2035.ru

МОДЕЛИ ТЕХНОЛОГИЧЕСКОГО СУВЕРЕНИТЕТА: ДРОНЫ И БЛИЖНИЙ КОСМОС VER. 2.0

МОДЕЛИ МЫШЛЕНИЯ

МОДЕЛЬ РЫНКА БАС

ТЕХНОЛОГИИ СВЯЗИ И УПРАВЛЕНИЯ

ЦИФРОВЫЕ СЕРВИСЫ

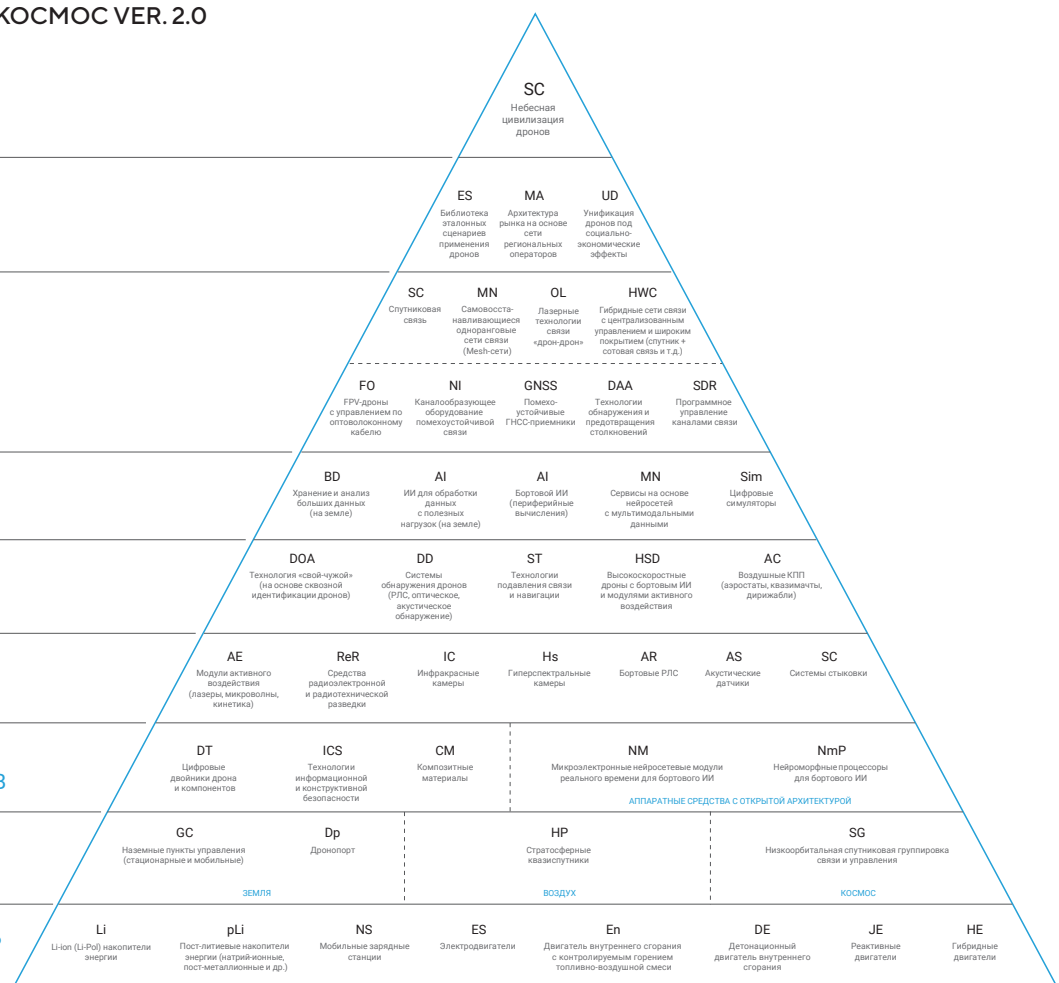
ТЕХНОЛОГИИ КОНТРОЛЯ НЕБА

ПОЛЕЗНЫЕ НАГРУЗКИ ДЛЯ ДРОНОВ

ПРОИЗВОДСТВО ДРОНОВ, СИСТЕМ И КОМПОНЕНТОВ

ИНФРАСТРУКТУРА УПРАВЛЕНИЯ

ЭНЕРГОООРУЖЕННОСТЬ ДРОНА



Как работает Модель
технологического суверенитета



смотреть
видео



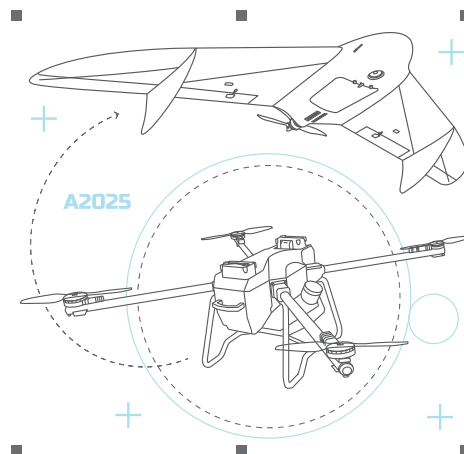
Станьте участником программы испытаний технологических решений для цифрового неба



Примите участие в стратегическом диалоге об освоении воздушного и космического пространства



Соберите вместе с участниками отрасли модель технологического суверенитета



Примите участие в проектно-образовательном интенсиве «Архипелаг 2025»:

- Лаборатория «Бесшовное Цифровое Небо»
- Соревнования дронов «Кибериммунная автономность»



Подписывайтесь на ТГ-канал «Настоящее Будущее»



**СИЛИНГ АНДРЕЙ
ЛЕОНАРДОВИЧ**

Исполнительный директор
АНО «Платформа НТИ»

Контакты:
a.siling@nti.work



**ТИХОНОВ АНДРЕЙ
ИВАНОВИЧ**

Президент ассоциации
«Доверенная платформа»

Контакты:
andrey.tikhonov@trustform.org







КИБЕРИММУНИТЕТ
ЦИФРОВОГО НЕБА



ПЛАТФОРМА НТИ

ФОНД НТИ

Доверенная
ПЛАТФОРМА