Аннотация – В последние годы Россия вступила на путь цифрового суверенитета, чему способствовало сочетание геополитической напряжённости, западных санкций и выбора внутренней политики. Этот сдвиг, ускоренный западными санкциями, привёл к значительной трансформации технологического ландшафта страны. По мере ухода западных компаний и ужесточения санкций Россия все чаще обращается к отечественным альтернативам и китайским технологиям, чтобы заполнить образовавшийся вакуум. В этой материале рассматривается растущий цифровой суверенитет России и растущая зависимость от китайских технологий, особенно в свете западных санкций. В нем исследуются последствия этого сдвига для прав человека в России, кибер-безопасности и международных отношений.

I. Призыв CFR к действию: оценка безопасности Astra Linux и цифрового суверенитета России

Совет по международным отношениям (CFR), известный аналитический центр США, призвал использовать разведывательные ресурсы для оценки безопасности российской операционной системы Astra Linux. Эта инициатива является частью более широкого исследования усилий России по импортозамещению и цифровому суверенитету. Astra Linux широко используется в российских военных и разведывательных системах, что делает её безопасность предметом интереса американских аналитиков.

CFR предполагает, что открытый исходный код Astra Linux может содержать уязвимости, которые могут быть использованы глобально. Они выступают за OSINT, чтобы понять, как в России внедряются технологии, подобные Astra Linux, и выявить потенциальные слабые места в системе безопасности. CFR также отмечает, что «растущая цифровая изоляция России и зависимость от отечественных и китайских технологий могут ограничить её доступ к мировому опыту в области кибер-безопасности, что потенциально повлияет на безопасность Astra Linux».

Astra Linux сертифицирована для использования в средах, требующих высокого уровня защиты данных, включая военные и правительственные учреждения. Несмотря на это, американский аналитический центр видит потенциальные возможности для использования уязвимостей из-за ограниченных ресурсов, доступных для тестирования и обеспечения безопасности системы по сравнению с западными аналогами.

Ключевые аспекты публикации CFR:

- **Позиция CFR**: CFR, хотя и претендует на статус независимой организации, имеет в своём совете директоров бывших офицеров разведки, журналистов и представителей бизнеса (включая финансового директора Alphabet).
- **Объект интереса**: Astra Linux широко используется в российских военных и разведывательных информационных системах.
- **Предлагаемый подход**: CFR призвал аналитиков в США и союзных странах использовать развед-данные с открытым исходным кодом, чтобы понять, как Россия внедряет технологии, подобные Astra Linux.
- **Потенциальные уязвимости**: CFR предполагает, что Astra Linux, основанная на программном обеспечении с открытым исходным кодом, может иметь уязвимости, которые можно использовать глобально.
- **Ограниченные ресурсы**: CFR утверждает, что у российских разработчиков может быть меньше ресурсов для всестороннего тестирования и защиты своего кода по сравнению с западными коллегами.

Разработчики Astra Linux, "Астра Груп", отреагировали на эти заявления:

- Они подчеркнули, что их продукт проходит тщательное тестирование и сертификацию.
- Компания посоветовала своим клиентам тщательно следовать рекомендациям по настройке системы безопасности и своевременно применять обновления для устранения потенциальных уязвимостей.
- "Астра Груп" заявила, что усилила меры по обнаружению вредоносных включений в своём программном обеспечении в связи с текущей международной ситуацией.

A. Голоса с цифрового рубежа: мнения экспертов о кибер- суверенитете России и Astra Linux

По мере того, как Россия прокладывает свой курс к цифровому суверенитету, хор голосов экспертов по кибер-безопасности, политических аналитиков и инсайдеров отрасли предлагает различные точки зрения на этот сложный ландшафт. Их выводы рисуют детальную картину

цифрового суверенитета России, потенциальных уязвимостей и сильных сторон Astra Linux, а также более широких последствий для глобальной кибер-безопасности. От опасений по поводу ограниченного доступа к международному опыту до проблем создания самоподдерживающейся экосистемы Интернета эти комментаторы проливают свет на многогранный характер технологического разворота России.

- **Джастин Шерман**, основатель и генеральный директор Global cyber Strategies, прокомментировал цифровую изоляцию России и её влияние на кибер-безопасность страны. Он упомянул, что растущая зависимость России от отечественных и китайских технологий может ограничить её доступ к мировому опыту в области кибер-безопасности, что потенциально повлияет на безопасность Astra Linux.
- **В статье The Security Affairs** обсуждаются планы российских военных заменить Windows на Astra Linux, ссылаясь на опасения по поводу возможного наличия скрытых бэкдоров в зарубежном программном обеспечении. Это подчёркивает снижение потенциальных рисков, связанных с использованием иностранных технологий. potential risks of relying on foreign technologies.
- **В статье Cybersec84** упоминается программа поиска ошибок Astra Linux, целью которой является выявление уязвимостей в операционной системе. Это говорит о том, что Astra Linux может обладать неизвестными возможностями для тестирования и защиты своего кода по сравнению с западными аналогами.
- **Исследование Margin Research,** посвящённое кибер-операциям России, подчёркивает растущее внимание страны к программному обеспечению с открытым исходным кодом, особенно к операционной системе Astra Linux, как части её стратегии по замене западных технологий и расширению своего глобального технологического присутствия

II. Опасения CFR: ограниченные возможности России по обеспечению безопасности Astra Linux в условиях цифровой изоляции

В последние годы Россия идёт по пути цифрового суверенитета, разрабатывая собственные технологии для снижения зависимости от западных продуктов. Ключевым компонентом этой стратегии является Astra Linux, отечественная операционная система, широко используемая в российских военных и разведывательных системах. Однако CFR выразил обеспокоенность по поводу потенциальных уязвимостей в этой системе.

Важно понимать, что эти опасения в значительной степени носят спекулятивный характер. Реальные возможности безопасности Astra Linux не являются общедоступными, и её разработчики утверждают, что приняты строгие меры безопасности. Тем не менее, анализ CFR выявляет несколько потенциальных недостатков, связанных с переходом к отечественным и китайским технологиям.

- **Ограниченные ресурсы**: CFR предполагает, что у российских разработчиков может быть меньше ресурсов для всестороннего тестирования и защиты своего кода по сравнению с западными коллегами. Потенциально это может привести к появлению нераскрытых уязвимостей.
- **Ограниченный доступ к глобальным специалистам в области кибер-безопасности**: Переходя на отечественную и китайскую продукцию, Россия может потерять доступ к экспертным знаниям в области кибер-безопасности из Соединённых Штатов, Западной Европы, Японии и других стран. Это может повлиять на общую безопасность системы, причём неожиданно в положительном ключе.
- **База с открытым исходным кодом**: Astra Linux основана на операционной системе с открытым исходным кодом. Хотя это позволяет настраивать и повышать надёжность, это также может привести к появлению уязвимостей, которые могут быть использованы глобально.
- **Независимость от мирового технологического сообщества**: растущая цифровая независимость России может ограничить её доступ к новейшим методам обеспечения безопасности (со встроенными бэкдорами и новыми каналами утечки данных?), инструментам и разведданным об угрозах, которыми делится мировое техническое сообщество.
- **Концентрация технологий**: Широкое внедрение Astra Linux в российских военных и разведывательных системах может создать ситуацию, при которой любые потенциальные уязвимости могут быть использованы в широком спектре критически важных объектов инфраструктуры.
- **Быстрая разработка и внедрение**: Стремление быстро разрабатывать и внедрять отечественные технологические решения может привести к поспешному внедрению систем безопасности или упущенным уязвимостям.
- **Менее разнообразная экосистема**: злоумышленникам, обнаружившим уязвимость, может быть проще ориентироваться на более однородную технологическую среду, в отличие от разнообразной экосистемы с несколькими операционными системами и версиями программного обеспечения.

III. Глобальный альянс по кибер-безопасности: США и союзники объединяются для оценки уязвимостей Astra Linux

По мере роста озабоченности по поводу безопасности российской операционной системы Astra Linux Соединённые Штаты не одиноки в своих усилиях по оценке потенциальных уязвимостей. Коалиция технологически союзников, каждый из которых обладает уникальным опытом и ресурсами, будет пытаться сыграть решающую роль в решении этой сложной задачи кибер-безопасности. От разведывательного альянса "Пять глаз" до членов НАТО и стратегических партнёров в Азии - эти международные усилия представляют собой огромный резерв талантов и ресурсов.

A. Обмен разведывательными данными и их анализ

- **Великобритания**: Являясь ключевым членом альянса Five Eyes, Великобритания предоставляет обширные возможности в области радиоразведки через британскую спецслужбу, отвечающую за ведение радиоэлектронной разведки и обеспечение защиты информации (GCHQ). Ее опыт в области криптографии и анализа данных особенно ценен.
- **Канада**: Управление по безопасности связи (CSE) предлагает передовые возможности для защиты критически важной инфраструктуры и анализа разведывательных данных из-за рубежа.
- **Австралия**: Австралийское управление связи (ASD) предоставляет значительный опыт в области киберзащиты и информацию о региональной разведке.

B. Технологические инновации

- **Япония**: Известная своим передовым технологическим сектором, Япония может предложить инновационные подходы к кибербезопасности, особенно в таких областях, как квантовые вычисления и обнаружение угроз с помощью искусственного интеллекта.
- **Южная Корея:** Благодаря своей передовой ИТ-инфраструктуре Южная Корея обладает опытом в обеспечении безопасности сетей 5G и устройств Интернета вещей (IoT).
- **Израиль**: Известный своей индустрией кибербезопасности, Израиль предоставляет передовые аналитические данные об угрозах и инновационные решения в области безопасности.

C. Стратегическая и оперативная поддержка

- **Члены НАТО**: Такие страны, как Франция, Германия и Нидерланды, предлагают различные точки зрения и могут внести свой вклад в единую стратегию кибербезопасности с помощью системы киберзащиты НАТО.
- **Новая Зеландия**: Несмотря на меньшие размеры, новозеландское бюро правительственной связи по безопасности (GCSB) предоставляет данные радиоэлектронной разведки и поддержку в области кибербезопасности.

D. Региональный опыт

- **Австралия и Япония**: обе страны предоставляют важную информацию о кибер-угрозах в Азиатско-Тихоокеанском регионе, расширяя глобальную перспективу коалиции.
- **Европейские партнёры**: члены НАТО могут обеспечить глубокое понимание кибер-проблем, с которыми сталкивается Европа, и потенциальной деятельности России в киберпространстве.

IV. Глобальный контроль и влияние Китая: меняющийся ландшафт цифрового суверенитета России

Поскольку Россия продолжает стремиться к цифровому суверенитету, в частности, посредством разработки и внедрения Astra Linux, международные организации и CFR внимательно следят за ситуацией. Такая тщательная проверка продиктована соображениями кибер-безопасности, экономическими интересами и растущим влиянием китайских технологий в России. Взаимосвязь между цифровой независимостью России, её растущей зависимостью от китайских технологий и потенциальными последствиями для глобальной кибер-безопасности тала предметом анализа.

- **Международный мониторинг Astra Linux:**
  - **Атлантический совет**: Опубликованы статьи и отчёты о цифровой изоляции России и разработке Astra Linux.
  - **Совет по международным отношениям**: проанализировал цифровую изоляцию России и развитие Astra Linux.
  - **Глобальные кибер-стратегии**: Опубликованы отчёты о цифровой изоляции России и Astra Linux.
- **Причины мониторинга:**
  - **Проблемы кибер-безопасности**: оценка потенциальных рисков в государственном и оборонном секторах.
  - **Экономические интересы**: оценка влияния на западные компании и рынки.
  - **Цифровая изоляция**: анализ влияния на глобальную кибер-безопасность и сотрудничество.
  - **Huawei и DJI**: смещение акцента на привлечение талантов и исследования и разработки в России.
- **Опасения CFR:**
  - **Риски кибер-безопасности**: потенциальные уязвимости в китайских продуктах.

- **Стратегический расклад**: зависимость России от Китая создаёт новую геополитическую динамику.
- **Экономические последствия**: Изменение структуры мировой торговли и динамики технологической отрасли.

V. Волновой эффект: глобальные последствия технологического расцвета Astra Linux

По мере того, как Россия продвигается вперёд в реализации своей программы цифрового суверенитета, возглавляемой разработкой и внедрением Astra Linux, глобальный технологический ландшафт переживает сейсмические сдвиги. Эта технологическая переориентация - не просто вопрос национальной политики; она вызывает каскад последствий, которые отражаются на международных рынках, геополитических альянсах и парадигмах кибер-безопасности. Технологический стержень России - от разрушения устоявшихся долей рынка до создания новых уязвимостей и возможностей - меняет цифровой мир таким, каким мы его знаем.

A. Сдвиг в динамике мировой технологической индустрии

- **Снижение доли рынка:**
  - Западные технологические гиганты, такие как Microsoft, Intel и Apple, теряют значительную долю рынка в России. Эта потеря доли рынка может повлиять на глобальные доходы и влияние этих компаний.
- **Фрагментация глобальной технологической экосистемы:**
  - Стремление России к технологическому суверенитету может вдохновить другие страны на разработку собственных внутренних альтернатив западным технологиям.
  - Эта тенденция может привести к более фрагментированному глобальному технологическому ландшафту, потенциально препятствуя функциональной совместимости и глобальному сотрудничеству в области развития технологий.

B. Уязвимости цепочки поставок

- **Зависимость от китайских технологий:**
  - Россия стала больше зависеть от китайских полупроводников и электроники и эта зависимость может создать потенциальные "точки отказа" в российской цепочке поставок, которыми могут воспользоваться западные страны.
- **Риски кибер-безопасности:**
  - Использование китайских технологий, которые, возможно, имеют известные уязвимости в системе безопасности, может привести к появлению новых рисков кибер-безопасности в российских системах.
  - Этой ситуацией потенциально могут воспользоваться западные спецслужбы или кибер-преступники.

C. Экономические последствия для Запада

- **Потеря российского рынка:**
  - Западные технологические компании потеряли доступ к российскому рынку, который ежегодно приносил миллиарды долларов.
  - **Microsoft**: Доходы Microsoft Rus значительно сократились в последние годы, составив 211,6 миллиона рублей в 2023 году по сравнению с 6,4 миллиарда рублей в 2022 году. Это указывает на резкое снижение их деловой активности в России.
  - **IBM**: Доход IBM в России в 2021 году составил около 300 миллионов долларов, и компания не ожидала доходов от российского рынка в 2022 году. Это свидетельствует о значительном сокращении их деловой активности в России.
  - **SAP**: SAP сообщила о снижении доходов в России на 50,8%, до 19,382 миллиарда рублей в 2022 году. Выход компании с российского рынка из-за геополитических событий значительно повлиял на ее финансовые показатели.
  - **Cisco**: Доходы Cisco в России снизились на 3,7% в 2021 году, с 37,1 миллиарда до 35,8 миллиарда рублей. Компания столкнулась с трудностями из-за геополитической напряжённости и санкций.
- **Изменение мировых торговых потоков:**
  - Переориентация российских технологических цепочек поставок с Запада на Китай меняет структуру мировой торговли в технологическом секторе.
  - Этот сдвиг потенциально может ослабить экономическое влияние Запада на Россию и укрепить глобальные экономические позиции Китая.
- **Проблемы игнорирования санкций:**
  - Использование стран-посредников и сложных цепочек поставок для обхода санкций создаёт проблемы для западных политиков и правоохранительных органов.
  - Эта ситуация может потребовать более изощренных и скоординированных усилий для поддержания эффективности санкций.

D. Долгосрочные стратегические последствия

- **Смена геополитического расклад сил:**

- Растущая технологическая зависимость России от Китая может изменить баланс сил в регионе и во всем мире.
- Этот сдвиг потенциально может ослабить влияние Запада и укрепить стратегическое партнёрство России и Китая.

- **Влияние на технологическую независимость России**:
  - Россия сделала шаг в сторону внутреннего производства, и переход от западных технологий к китайским, что может иметь долгосрочные стратегические последствия.
- **Гонка технологических инноваций:**
  - Фрагментация глобальной технологической экосистемы может привести к параллельному развитию технологий, потенциально ускоряя инновации в некоторых областях, но также приводя к несовместимым стандартам и системам.

E. Возможности для западной политики

- **Использование уязвимостей:**
  - CFR предполагает, что западные страны могли бы выявить и потенциально использовать уязвимости в новой технологической экосистеме России, особенно в областях, где российские системы полагаются на китайские технологии.
- **Укрепление альянсов:**
  - Запад будет использовать эту ситуацию для укрепления технологических и экономических союзов с другими странами, потенциально изолируя Россию и Китай в определённых технологических секторах.
- **Продвижение открытых стандартов:**
  - Западные страны могли бы продвигать открытые, совместимые стандарты в новых технологиях, чтобы противостоять тенденции к фрагментации и сохранить глобальное технологическое лидерство.
- **Технологические риски, связанные с международным использованием Astra Linux -** в основном связаны с попытками предотвратить его распространение на западных рынках.
- **Проблемы совместимости:**
  - Индивидуальные особенности Astra Linux могут не интегрироваться беспрепятственно с международным программным обеспечением и оборудованием.
  - Это может привести к значительным проблемам совместимости.
- **Ограниченная поддержка:**
  - Из-за ограниченной международной поддержки пользователи могут столкнуться с трудностями в доступе к помощи и ресурсам, когда это необходимо.
  - Это ограничение может затруднить способность западных технологических экосистем адаптироваться к разнообразным операционным системам.
- **Влияние на сотрудничество и инновации:**
  - Предотвращение распространения Astra Linux может ограничить возможности для сотрудничества и инноваций.
  - Разнообразные технологические среды обычно более устойчивы и способствуют инновациям.
- **Повышенная уязвимость кибербезопасности:**
  - Зависимость от одного источника технологий может увеличить уязвимость к киберугрозам.
  - Взаимодействие с Astra Linux может помочь западным рынкам понять и смягчить потенциальные риски безопасности.

VI. Защита Astra Linux от шпионажа

В постоянно меняющемся мире кибер-безопасности Astra Linux является России в борьбе с цифровым шпионажем. Поскольку страна стремится к технологической независимости, важность надёжных мер по борьбе со шпионажем трудно переоценить. Стратегия защиты Astra Linux включает в себя многогранный подход, сочетающий передовые технологии со строгими протоколами для защиты конфиденциальной информации. Эта комплексная система не только защищает от внешних угроз, но и устраняет внутренние уязвимости, создавая надёжную защиту от промышленного шпионажа и кибер-атак.

Ниже приведены ключевые компоненты антишпионского арсенала Astra Linux:

- **Управление рисками**: Регулярная оценка, связанная с коммерческими секретами и конфиденциальной информацией с определением потенциальных угроз и уязвимости, чтобы для формирования понимания кого могут заинтересовать данные и как они могут попытаться получить к ним доступ.
- **Безопасная инфраструктура**: многоуровневый подход к обеспечению безопасности для защиты вашей сети и данных включает в себя установление безопасного периметра брандмауэров и внедрение модели нулевого доверия, при которой доступ проверяется на каждом этапе.
- **Ограничение доступа**: ограничение доступа к конфиденциальной информации с использованием

физических и технологических барьеры для ограничения доступа к коммерческой тайне.

- **Обучение сотрудников**: информирование сотрудников и подрядчиков о важности защиты коммерческой тайны и распознавания потенциальных угроз шпионажа.
- **Мониторинг и расследование**: Постоянный мониторинг на предмет несанкционированного доступа или подозрительных действий с последующим расследованием любых подозрений в шпионаже или утечке данных для уменьшения потенциального ущерба.
- **Физическая безопасность**: Защита физических местоположений и активов, содержащих конфиденциальную информацию, включает в себя безопасное хранение документов и мониторинг физических точек доступа.
- **Использование технологий**: использование передовых технологий кибер-безопасности, таких как системы обнаружения вторжений, шифрование и безопасные каналы связи, для защиты цифровой информации от кибер-шпионажа.
- **Защита коммерческой тайны**: политики и процедуры, специально разработанные для защиты коммерческой тайны и проведение регулярных аудитов для обеспечения соответствия протоколам безопасности.
- **Соглашения о неразглашении (NDA)**: требование от сотрудников, подрядчиков и партнёров подписания NDA, юридически обязывающих их не разглашать конфиденциальную информацию.