ЦИФРОВЫЕ КОЛЛАПСЫ. ЕСТЬ ЛИ ГАРАНТИИ НАДЕЖНОСТИ

Конспект встречи создан при помощи искусственного интеллекта и Яндекс Телемоста

ЦИАТИМ × Яндекс 360

20 МАЯ 2026

МОДЕРАТОР

Зызо Людмила, Заместитель директора РИЦ ТАСС Урал, ТАСС

УЧАСТНИКИ

• Балашов Демид, Руководитель по развитию продуктов кибербезопасности, МегаФон ПроБизнес

• Касперская Наталья, Президент, ГК Инфовотч

• Лукацкий Алексей, Киберцарь, Positive Technologies

• Поладьев Денис, Директор по информационной безопасности, АО "ЦХД"

• Шойтов Александр, Заместитель Министра, Минцифры России

• Обухов Александр, Генеральный директор, Турбо Облако

• Ставцев Роман, Руководитель дирекции по проектам «Базальт СПО»

• Лавров Андрей, Генеральный директор, АО "Гринатом"

• Прорубщиков Сергей, Исполнительный директор, АО «Интегро Текнолоджис»

Сессия на форуме ЦИПР объединила экспертов для обсуждения уязвимостей цифровой инфраструктуры и путей повышения ее устойчивости. Участники пришли к консенсусу, что абсолютных гарантий безопасности не существует, но риски можно минимизировать через многослойную защиту, резервирование и переход от концепции «защиты» к концепции «киберустойчивости». Ключевыми вызовами названы дефицит квалифицированных кадров, противоречия между интересами бизнеса и государства, а также риски, связанные с быстрым внедрением новых технологий, таких как искусственный интеллект.

Шойтов Александр (Минцифры России) открывает дискуссию, разделяя устойчивость на техническую работоспособность и защиту от кибератак. Он подчеркивает, что безопасность должна закладываться на этапе проектирования, а не добавляться постфактум, и указывает на проблему отсутствия единого национального игрока, способного обеспечить комплексную защиту всех отраслей. «Нужно консолидировать лучших специалистов и создать единую программу исследования безопасности для новых технологий под государственным крылом», – резюмирует он, отмечая, что ИИ ускоряет поиск уязвимостей злоумышленниками.

Наталья Касперская (ГК Инфовотч) утверждает, что человечество не придумало ничего нового в защите, кроме дублирования систем и мониторинга, но добавляет важный контекст геополитического противостояния. Она приводит пример атаки на «Аэрофлот», показавший, что критически важна не только защита, но и скорость восстановления после инцидента.

«Внедрение новых технологий – это вещь, противоположная безопасности, так как новое означает неисследованное», – предупреждает эксперт, призывая не спешить с внедрением инноваций на критических производствах без должного анализа рисков.

Алексей Лукацкий (Positive Technologies) указывает на фундаментальное рассинхронизирование интересов бизнеса, стремящегося к экономии, и государства, заботящегося о нацбезопасности. По его словам, это приводит к тому, что компании вынуждены строить «план Б» самостоятельно, так как государственные обещания часто меняются. «Надеяться на государство полезно, но рассчитывать, что в критический момент останешься только ты один, и никто не поможет, – реалистичный сценарий», – заключает он, отмечая острый дефицит архитекторов, способных проектировать отказоустойчивые системы.

Денис Поладьев (АО "ЦХД") акцентирует внимание на том, что киберустойчивость становится базовой IT-гигиеной, а не просто надстройкой. Он рекомендует подчинять службу информационной безопасности напрямую генеральному директору для обеспечения паритетных отношений с IT-подразделениями. «Мы провели киберучения на двух уровнях: техническом и на уровне штаба компании, чтобы отработать взаимодействие и коммуникации», — делится опытом спикер, подчеркивая важность сквозных процессов Security Design.

Александр Обухов (Турбо облако) анализирует надежность облачных сервисов, указывая на критическую проблему географической концентрации дата-центров в Москве. Он предлагает внедрять геораспределенность и мультиоблачные стратегии, чтобы избежать зависимости от одного провайдера. «Экономически эффективно строить собственный ЦОД сейчас становится сложнее, порог входа растет, поэтому использование внешних облаков становится необходимостью для дублирования», – объясняет он, добавляя, что суверенитет облака требует не только импортозамещения, но и контроля над акционерами.

Роман Ставцев (Базальт СПО) выступает за полную локализацию разработки операционных систем и построение экосистем на их базе. Он считает, что устойчивость инфраструктуры зависит от качества базового уровня, и предлагает развивать открытое ПО для создания независимых решений. «Локализация воспроизводимой разработки – это базовый подход, позволяющий жить дальше в случае отрезания от внешнего мира», – говорит он, отмечая важность доверия пользователей к длительности поддержки таких систем.

Демид Балашов (Мегафон) описывает телеком-отрасль как основу цифровой экономики, где сбой может привести к системному коллапсу. Он вводит понятие «эшелонированной защиты» и переключения фокуса с активной киберзащиты на пассивную киберустойчивость. «Задача телеком-оператора — обеспечивать целостно защищенную среду для клиентов, так как каждый клиент является точкой входа как в нашу систему, так и в систему контрагентов», – подчеркивает он, призывая к комплексному подходу на уровне всей цепочки поставок.

В финальном блиц-опросе участники предлагают конкретные шаги. **Алексей Лукацкий (Positive Technologies)** настаивает на проведении краш-тестов сценариев коллапсов, Наталья Касперская – на пересмотре политики инноваций в пользу взвешенного внедрения, а **Денис Поладьев (АО "ЦХД")** – на легализации программ вознаграждения за уязвимости. **Александр Обухов (Турбо облако)** советует бизнесу делать ставку на резервирование и георасределенность, а **Демид Балашов (Мегафон)** напоминает о важности цифровой гигиены для широких масс сотрудников...