ЦИПР | ЦИФРОВОЙ МАРКЕТПЛЕЙС

ЦИПР-2026 · АНАЛИТИКА

Кибербезопасность и киберустойчивость КИИ

От защиты периметра к устойчивости под огнём: обзор по материалам ЦИПР-2026

Нижний Новгород · май 2026

cipr.ru · platforms.su

Оглавление

1. Краткое резюме и ключевые выводы

На ЦИПР-2026 тема кибербезопасности и киберустойчивости КИИ охватила шесть сессий: партнёрские сессии РБК и Инфосистемы Джет, сессии по международным киберучениям ОДКБ+, M&A в кибербезопасности, реальной проверке киберустойчивости, партнёрскую сессию Т-Банк и трек по новой архитектуре ИТ/ИБ. В совокупности они дали срез актуальной угрозы для операторов КИИ, практики восстановления после инцидентов и нарождающегося рынка киберстрахования.

1. **Промышленность вышла на первое место среди атакуемых отраслей. По данным исследования, промышленный сектор обогнал финансовый; в 80+ процентах инцидентов используется вредоносное ПО по классическим схемам, каждый третий инцидент вызывает остановку бизнес-процессов (Новиков Алексей, Positive Technologies).**

2. **Более 75% атак приходится на объекты КИИ. Эту долю зафиксировало АльфаСтрахование по собственной страховой статистике; стоимость аренды необнаруживаемого вредоносного ПО составляет всего $400 (Скворцов Владимир, АО АльфаСтрахование; Новиков Алексей, Positive Technologies).**

3. **Парадигма смещается от «защиты» к «устойчивости». Ключевой вопрос теперь не «произойдёт ли атака», а «как быстро компания восстановится после неё» – этот сдвиг зафиксировали одновременно несколько спикеров из ВСК, Минцифры и Т-Банка (Фролов Роман, Страховой Дом ВСК; Хасин Евгений, Министерство цифрового развития, связи).**

4. **Time to exploit сократился с лет до дней, к 2027 году прогнозируются минуты. ИИ-инструменты ускоряют разведку и эксплуатацию уязвимостей до machine-speed; ожидание патча три дня уже означает компрометацию (Гадарь Дмитрий, ТБанк).**

5. **Реальный рынок киберстрахования в России – менее 1 млрд руб., что составляет менее 0,1% российского страхового рынка; мировой рынок по данным Munich Re достиг 14–15 млрд долл. в 2024 году и прогнозируется более 100 млрд долл. к 2028 году (Фролов Роман, Страховой Дом ВСК; Богданов Валентин, ООО «УЦСБ»; Еремеев Иван, РК Страховой Брокер).**

6. **Подрядчики – основной вектор проникновения в крупные организации. По статистике Инфосистем Джет, более 50% проникновений в крупных компаниях идёт через подрядчиков; общая статистика даёт ~10% (Елисеев Владимир, ИНФОСИСТЕМЫ ДЖЕТ; Фролов Роман, Страховой Дом ВСК).**

7. **BCP-план, не проверенный учениями, примерно наполовину нерелевантен при реальной атаке. Этот вывод сделан ВСК по итогам инцидента ноября 2025 года; ТМК провела двухнедельные корпоративные учения с вовлечением генерального директора, выявившие расхождения между планами и реальностью (Фролов Роман, Страховой Дом ВСК; Якоб Дмитрий, ПАО «ТМК»).**

8. **ИИ-агенты автоматизируют как атаки, так и защиту. Система Nula (ТБанк) выполняет за 15–20 минут работу, на которую у топовых инженеров уходит 2–3 суток; 87% респондентов глобальных опросов назвали уязвимости ИИ главным быстрорастущим риском 2025 года (Гадарь Дмитрий, ТБанк).**

9. **Россия масштабирует международные киберучения ОДКБ+ с прицелом на ООН. На ЦИПР-2026 подведены итоги первого этапа: 26 команд из 8 стран отработали реагирование при атаках на инфраструктуру СМИ; следующий этап планируется под эгидой ООН (Шойтов Александр, Минцифры России; Люкманов Артур, МИД России).**

10. **Российский рынок кибербезопасности растёт на 20–30% в год, но составляет лишь 1,5–2% мирового. На рынке около 300 компаний, из которых инвестиционный интерес представляют ~10%; крупнейшая сделка – СП SolidLab и «Яндекс» 50/50 (Попов Егор, Sk Capital; Железняков Вячеслав, Группа компаний SolidLab).**

2. Контуры темы: шесть сессий, единая повестка

Кибербезопасность КИИ на ЦИПР-2026 охватила шесть тематических блоков – от угроз и практики реагирования до страхования, M&A и международной кооперации. Каждая сессия дала самостоятельный угол зрения, вместе они складываются в полноценный срез отрасли.

2.1 «Кибербезопасность как новая роскошь ответственного бизнеса»

Партнёрская сессия РБК (19 мая) собрала представителей Минцифры, Positive Technologies, АльфаСтрахования, Медси, Росатома и Билайна. Центральный тезис – кибербезопасность является базовым минимумом, а не роскошью; те, кто годами копил кибертехнологический долг, теперь платят за него кратно. Сессия дала данные об угрозах для промышленности и первый публичный отчёт о страховых случаях АльфаСтрахования.

2.2 «Непрерывность бизнеса в эпоху цифрового терроризма»

Партнёрская сессия Инфосистемы Джет (19 мая) разобрала реальный инцидент в ВСК: полное шифрование инфраструктуры, уничтожение резервных копий, три недели восстановления. Ключевые спикеры – ВСК, ТВЭЛ, ТМК, СОГАЗ. Именно здесь был введён термин «киберустойчивость» как операционная характеристика, а не «киберзащита».

2.3 «КИБЕРУЧЕНИЯ ОДКБ+. Подведение итогов»

Сессия 19 мая подвела итоги первого этапа международных учений: 26 команд из 8 стран – Россия, Беларусь, Казахстан, Венесуэла, Мьянма, Лаос, Буркина-Фасо и Эфиопия. Организаторы – МГТУ им. Баумана и ГК «ГИЗ» при поддержке Минцифры, НКЦКИ и МИД РФ.

2.4 «M&A в кибербезопасности. Новые горизонты защиты реального сектора»

Сессия третьего дня ЦИПР-2026 (20 мая) посвящена структуре сделок и барьерам для инвестиций в российский рынок кибербезопасности. Спикеры – CICADA8, Start X, SolidLab, CyberED, Sk Capital, Базис.

2.5 «Реальная проверка киберустойчивости и киберстрахование в технологическом и промышленном секторе»

Сессия первого дня (18 мая) сопоставила практику пентестов и red team с состоянием рынка киберстрахования. Ключевые спикеры – ВСК, УЦСБ, РК Страховой Брокер, Северсталь, Гарда, Инфовотч, АльфаСтрахование, АЙДЕКО.

2.6 «Гонка скоростей» и «Новая архитектура ИТ/ИБ»

Две сессии 18 и 19 мая рассмотрели угрозу machine-speed атак, роль ИИ-агентов в наступательной и оборонительной безопасности, а также переход к архитектуре Security by Design. Спикеры – ТБанк, Норникель, Аэрофлот, CLOUD.RU, СберТех, ГК «Солар», МТС WEB SERVICES, Минцифры.

3. Промышленность под ударом: угрозы и векторы атак на КИИ

По данным, прозвучавшим на ЦИПР-2026, промышленные предприятия и операторы КИИ стали главной мишенью киберпреступников. Данные Positive Technologies зафиксировали структурный сдвиг в целеполагании атакующих.

3.1 Промышленность – отрасль №1 по числу атак

По данным Positive Technologies, промышленность вышла на первое место среди атакуемых отраслей, обогнав финансовый сектор. В 80+ процентах инцидентов в промышленности применяется вредоносное ПО по классическим схемам; социальная инженерия остаётся значимым вектором. Каждый третий инцидент вызывает остановку бизнес-процессов (Новиков Алексей, Positive Technologies).

По данным АльфаСтрахования, более 75% атак приходится именно на предприятия – операторы объектов КИИ (Скворцов Владимир, АО АльфаСтрахование).

3.2 Низкая стоимость входа для атакующих

Аренда вредоносного ПО, не определяемого ни одним антивирусом, стоит $400 – «копейки», по оценке Positive Technologies. Это означает, что барьер входа для атакующих практически отсутствует, тогда как стоимость инцидента для жертвы исчисляется десятками и сотнями миллионов рублей (Новиков Алексей, Positive Technologies).

3.3 Кибершпионаж как скрытая угроза

Новиков Алексей (Positive Technologies) выделил кибершпионаж как недооценённый класс угроз: злоумышленники могут годами незаметно читать корпоративную переписку, знать переговорные позиции и планы компании. Финансовый ущерб от такого

присутствия невидим, но реален.

3.4 Атаки через цепочку подрядчиков

По статистике Инфосистем Джет, более 50% проникновений в крупных организациях происходит через внешних подрядчиков – атаковать их инфраструктуру проще, чем напрямую взламывать крупную компанию (Елисеев Владимир, ИНФОСИСТЕМЫ ДЖЕТ). Шойтов Александр (Минцифры России) также назвал атаки через подрядчиков в числе ключевых вызовов. Валентин Богданов (ООО «УЦСБ») подчеркнул, что компании недооценивают именно этот вектор.

3.5 ИИ ускоряет и удешевляет атаки

Генеративный ИИ делает атаки «более дешёвыми, быстрыми и полными»; таргетированный фишинг с применением ИИ становится массовым явлением (Шойтов Александр, Минцифры России). Модель Anthropic Mythos Cloud Preview нашла более 1000 уязвимостей во всех основных операционных системах и браузерах (Гадарь Дмитрий, ТБанк). SOC ТМК фиксирует несколько тысяч атак в месяц только на первой линии (Якоб Дмитрий, ПАО «ТМК»).

4. От киберзащиты к киберустойчивости: смена парадигмы

Центральная идея, сформулированная сразу несколькими сессиями ЦИПР-2026, – отказ от иллюзии полной защиты в пользу способности быстро восстановиться. Это не компромисс, а новая операционная реальность.

4.1 Assume breach как исходная позиция

Хасин Евгений (Министерство цифрового развития, связи) прямо назвал смену цели: «Защита никогда не сможет обеспечить стопроцентную гарантию, что ни одна атака не пройдёт. Но защита должна быть готова к тому, чтобы устранить последствия атак». Новый приказ ФСТЭК, вступивший в силу в марте 2026 года, закрепляет обязательные этапы инвентаризации активов и анализа защищённости.

Фролов Роман (Страховой Дом ВСК) ввёл понятие «киберустойчивость» как характеристику скорости восстановления: «вопрос не если, а вопрос когда».

4.2 Security by Design вместо периметра

Гадарь Дмитрий (ТБанк) констатировал: «Защищаться привычными способами классической безопасности может оказаться вредно для безопасности. Нужно синергично вместе с IT выстраивать другую архитектуру безопасности». Соколов Андрей (АО ГК «МЕДСИ») добавил: «Раньше мы жили "сначала построим, а потом будем защищать". Сейчас уже это невозможно».

4.3 ИИ-агенты на стороне защиты

ТБанк развернул систему атакующих ИИ-агентов Nula, которая в автономном режиме круглосуточно тестирует собственную инфраструктуру. Задача, занимающая у топовых инженеров 2–3 суток, выполняется за 15–20 минут. ТБанк также объявил переход к открытой программе кибериспытаний с выплатой 12 млн руб. за одно подтверждённое событие с июня 2026 года (Гадарь Дмитрий, ТБанк).

4.4 Измерение как основа прогресса

Новиков Алексей (Positive Technologies) предложил конкретную стратегию: «от медведя не надо убегать первым» – достаточно быть защищённее, чем сосед по отрасли. Это требует регулярного измерения уровня защищённости в разрезе отраслевого сегмента. Когда каждый начнёт измеряться, уровень защищённости всей отрасли поднимется настолько, что атакующие предпочтут переместиться в другие страны.

4.5 Бюджетный дисбаланс

В ТВЭЛ 80% бюджета информационной безопасности уходит на предотвращение атак и лишь 20% – на готовность к восстановлению. Гаранин Евгений (АО «ТВЭЛ») назвал это структурной проблемой: построить абсолютно непроницаемую инфраструктуру невозможно при скорости изменения ИТ-ландшафта в 30–40% в год (Гаранин Евгений, АО «ТВЭЛ»).

5. Реальные инциденты: кейсы и уроки

На ЦИПР-2026 несколько компаний впервые публично раскрыли детали собственных крупных инцидентов. Эти кейсы – наиболее ценная часть программы, поскольку в публичное поле попадает менее 10% информации о реальных кибератаках.

5.1 Кейс ВСК: три недели без инфраструктуры

11 ноября прошлого года Страховой Дом ВСК подвергся одной из крупнейших кибератак на российском рынке. Злоумышленники компрометировали учётные записи через подрядчика, зашифровали всю виртуальную инфраструктуру на обоих ЦОД и уничтожили резервные копии. Компания полностью восстановилась за три недели, однако восемь недель практически без выходных работала над ликвидацией последствий (Фролов Роман, Страховой Дом ВСК).

Буквально накануне атаки – 10 ноября – правление ВСК отклонило дополнительный бюджет на кибербезопасность в 100 млн руб. как нереалистичный. По итогам инцидента текущие затраты компании на ИБ составляют около 30–40% от понесённых потерь от атаки. Роль CISO была повышена до члена правления (Фролов Роман, Страховой Дом ВСК).

5.2 Кейс ТМК: учения как прививка

ПАО «ТМК» провело масштабные двухнедельные корпоративные DR-учения в боевом режиме с вовлечением генерального директора; подготовка к ним заняла до полугода. Якоб Дмитрий (ПАО «ТМК») признал, что учения выявили расхождения между

задокументированными планами и реальным положением дел. SOC ТМК фиксирует несколько тысяч атак в месяц на первой линии.

5.3 Кейс Аэрофлота: реальный инцидент и отраслевая кооперация

Денис Попов (ПАО «Аэрофлот») подтвердил опыт реального инцидента и описал усиление SOC через дочернюю структуру AFLT Systems. Транспортная отрасль обсуждает создание отраслевого центра кибербезопасности из-за высокой взаимосвязанности участников (Попов Денис, ПАО «Аэрофлот»).

5.4 Кейс Ирана: 70 дней под непрерывными атаками

Представитель цифрового банка Парсиан (Иран) поделился опытом 70 дней непрерывных атак интенсивностью более 1000 в сутки на банковский сектор страны. Ни одна атака не прошла успешно – защита была обеспечена не изоляцией, а обменом информацией между государством и частными компаниями в режиме реального времени (Джавади Мехди, цифровой банк Парсиан, через переводчика).

6. Киберстрахование как инструмент управления риском

Рынок киберстрахования в России находится на самых ранних стадиях зрелости, однако первые реальные страховые случаи уже зафиксированы. Сессии ЦИПР-2026 дали наиболее подробную из публично доступных картин этого рынка.

6.1 Объём и зрелость российского рынка

Реальный объём корпоративного киберстрахования в России составляет менее 1 млрд руб. – менее 0,1% страхового рынка страны (Фролов Роман, Страховой Дом ВСК; Богданов Валентин, ООО «УЦСБ»; Еремеев Иван, РК Страховой Брокер). За последние два года на российском рынке урегулировано лишь около 8 страховых случаев; крупнейшая выплата превысила 200 млн руб., вторая – чуть больше 50 млн руб., большинство остальных – в диапазоне 20–30 млн руб. Максимальный лимит покрытия, который сейчас готовы предоставлять страховщики, – до 3 млрд руб. (Еремеев Иван, РК Страховой Брокер).

6.2 Мировой рынок: кратный разрыв

По данным Munich Re, мировой рынок киберстрахования составил 14–15 млрд долл. в 2024 году и 20–22 млрд долл. по прогнозу на 2025 год. К 2028 году ожидается рост до более 100 млрд долл. Российский прогноз – 10 млрд руб. к 2027–2028 году (Фролов Роман, Страховой Дом ВСК; Богданов Валентин, ООО «УЦСБ»).

6.3 Барьеры: взаимное недоверие и пустой рынок

Хайретдинов Рустэм (Гарда) охарактеризовал главную проблему как взаимное недоверие: страховщики опасаются мошенничества, клиенты убеждены, что страховая найдёт повод не платить. Страховщики не умеют оценивать киберриски так же, как традиционные риски, что ведёт к завышенным ставкам или отказам от покрытия.

6.4 Импортозамещение как фактор тарифообразования

Арефьев Андрей (ГК Инфовотч) предложил нестандартный подход: страховщикам целесообразно предоставлять пониженные ставки компаниям, завершившим импортозамещение, поскольку используемый ими стек контролируется отечественными компаниями и имеет более предсказуемый профиль риска (Арефьев Андрей, ГК Инфовотч).

6.5 Киберстрахование как сервис, а не финансовая подушка

Фролов Роман (Страховой Дом ВСК) назвал ключевым сдвигом переход от понимания киберстрахования как финансовой компенсации к сервисной модели: страховщик должен обеспечивать оперативное реагирование на инцидент, а не просто выплачивать деньги после него. АльфаСтрахование подписало партнёрское соглашение с Positive Technologies именно для оперативного реагирования (Фролов Роман, Страховой Дом ВСК; Скворцов Владимир, АО АльфаСтрахование).

7. ИИ в арсенале атакующих и защитников

Искусственный интеллект стал центральной темой в контексте киберугроз – одновременно как инструмент атакующих и как потенциальный ответ защитников. Спикеры ЦИПР-2026 зафиксировали и конкретные применения, и системные риски.

7.1 ИИ на стороне атакующих

Шойтов Александр (Минцифры России) описал угрозу генеративного ИИ: современные LLM-модели способны действовать как «полноценный хакер», делая атаки «более дешёвыми, быстрыми и полными». Таргетированный фишинг с применением ИИ становится массовым. Программы распознавания дипфейков достигают точности 90–95% в зависимости от качества материала (Шойтов Александр, Минцифры России).

Бобыльков Виктор (MTC WEB SERVICES) констатировал: «Сейчас искусственный интеллект информационной безопасности доставляет проблем больше, чем приносит пользы» – неконтролируемые утечки корпоративных данных через публичные LLM-сервисы (DeepSeek, Anthropic, ChatGPT) уже стали реальностью.

7.2 Time to exploit: дни становятся минутами

Гадарь Дмитрий (ТБанк) зафиксировал ключевой тренд: в 2026 году time to exploit – уже дни, тогда как в 2000-х это были годы. Прогноз на 2027 год – минуты. Ожидание патча три дня становится равнозначным отказу от защиты. Модель Anthropic Mythos Cloud Preview уже нашла более 1000 уязвимостей во всех основных ОС и браузерах.

7.3 ИИ-агенты в наступательной безопасности

ТБанк создал и эксплуатирует группу атакующих агентов Nula – автономную систему, которая круглосуточно взламывает собственные системы банка, выполняя за 15–20 минут задачи, на которые у топовых инженеров уходят 2–3 суток. Концепция non-human identity – временных учётных записей с минимальным набором прав для каждого агента –

названа наиболее недооценённым направлением безопасности (Гадарь Дмитрий, ТБанк).

7.4 Ответ регулятора и отрасли

Минцифры России рекомендует использовать равноценный ИИ для самооценки уязвимостей – «поставить его на стражу». CLOUD.RU внедряет autoresponse и autodeploy в SOC при текущем уровне роботизации 20%; Мартынцев Алексей (ПАО «ГМК «Норильский никель»») создал security data lake для прогнозирования атак на АСУ ТП (Шойтов Александр, Минцифры России; Волков Сергей, CLOUD.RU; Мартынцев Алексей, ПАО «ГМК «Норильский никель»»).

8. Международное измерение: ОДКБ+, ООН и кооперация CERT

На ЦИПР-2026 впервые публично подведены итоги международных киберучений ОДКБ+ – наиболее масштабного многостороннего мероприятия в сфере практической кибербезопасности под руководством России.

8.1 Итоги первого этапа киберучений ОДКБ+

В рамках председательства России в ОДКБ проведён первый этап серии отраслевых учений. Участвовали 26 команд из 8 стран: Россия, Беларусь, Казахстан, Венесуэла, Мьянма, Лаос, Буркина-Фасо, Эфиопия. Сценарий – реалистичная цепочка атак на инфраструктуру информационного агентства. Лидеры по результатам (по 16 баллов): Министерство науки и технологий Венесуэлы, ЗАО «Патио» (Беларусь), МИА «Россия сегодня» (Россия). Организаторы – МГТУ им. Баумана и ГК «ГИЗ» при поддержке Минцифры, НКЦКИ и МИД РФ.

8.2 Уроки, зафиксированные НКЦКИ

Анатолий Грачев (НКЦКИ) выделил три ключевых урока учений: необходимость осведомлённости владельцев критических систем о существовании уполномоченных организаций (CERT) в своих странах; способность национальных CERT договариваться о нейтрализации источника атаки; важность сбора объективных технических данных об атаке как основы любого реагирования.

8.3 Масштабирование под эгидой ООН

Артур Люкманов (МИД России) обозначил следующий шаг: масштабирование учений под эгидой ООН с использованием глобального межправительственного реестра контактных пунктов, функционирующего в ООН с 2024 года. Предыдущие учения прошли в Ханое в октябре 2025 года: 24 команды из 10 стран. Протоколы Консультационного координационного центра ОДКБ по реагированию на инциденты применяются уже более 10 лет.

8.4 Кооперация как условие успеха

Гадарь Дмитрий (ТБанк) сформулировал принципиальную позицию: «Я не вижу, что информационная безопасность – это область конкуренции компаний». Мартынцев Алексей (ПАО «ГМК «Норильский никель»») описал платформу БИБ-клуб (~100 компаний), созданную совместно Норникелем и Северсталью для обмена данными об инцидентах. Опыт Ирана – 70 дней без прорывов при более 1000 атак в сутки – был достигнут именно через государственно-частный обмен информацией (Гадарь Дмитрий, ТБанк; Мартынцев Алексей, ПАО «ГМК «Норильский никель»»).

9. Рынок кибербезопасности: инвестиции, M&A и консолидация

Сессия по M&A третьего дня ЦИПР-2026 дала редкую картину инвестиционного климата в российской кибербезопасности – с оценками мультипликаторов, описанием реальных сделок и взглядами основателей независимых стартапов.

9.1 Глобальный контекст и место России

Мировой рынок венчурного финансирования кибербезопасности достиг 14–18 млрд долл. в 2025 году (рекорд – 20 млрд долл. в 2021 году); 80% сосредоточено в США и Израиле (Шадюк Александра, АО Кибердом). Российский рынок кибербезопасности растёт на 20–30% в год – быстрее мирового (около 10% в год), – однако составляет лишь 1,5–2% мирового объёма (Попов Егор, Sk Capital).

На российском рынке насчитывается около 300 компаний, из которых инвестиционный интерес представляют ~10% (около 30 компаний). Целевая доходность SK Capital в кибербез-компаниях – 25–30%+ (Попов Егор, Sk Capital).

9.2 Реальные сделки

Железняков Вячеслав (Группа компаний SolidLab) описал СП 50/50 с «Яндексом»: сделка обеспечила технологическую синергию (on-premise SolidLab + облачные технологии Яндекса + ИИ) при сохранении полного операционного управления. Богомолов Егор (CyberED) рассказал о партнёрстве с фондом Cyber/Cyberus: получение каналов продаж и GR-экспертизы, выход на экспорт – обучение 4000 человек в одной из африканских стран, продажи в страны АСЕАН.

CICADA8 получала предложение о покупке на «n миллиардов рублей», но отказалась, сделав ставку на монопродуктовый рост в нише deception (Кузнецов Алексей, CICADA8).

9.3 Настроения основателей

Кузнецов Алексей (CICADA8) признал, что монопродуктовый стартап скорее всего будет поглощён крупным игроком в горизонте 3–5 лет. Тимурзиев Руслан (Базис) констатировал: «Эпоха апсайдов прошла. Наступила эра дисконтов». Попов Егор (Sk Capital) охарактеризовал часть продавцов как «космонавтов», мыслящих категориями десятикратных мультипликаторов при реальности российского рынка – 1,5–2% от мирового.

10. Игроки темы: компании и спикеры ЦИПР-2026

В рамках шести сессий по кибербезопасности КИИ на ЦИПР-2026 выступили более 40 спикеров из государственных структур, крупнейших промышленных и финансовых компаний, страховщиков и специализированных игроков рынка ИБ.

Государственные структуры и регуляторы

- **Минцифры России – Шойтов Александр (заместитель Министра) обозначил государственную позицию по ключевым вызовам: ИИ-угрозы, таргетированный фишинг, новые регуляторные требования ФСТЭК. Также представлены итоги антифрод-платформы (>98% заблокированных звонков, данные Билайна).**
- **МИД России – Люкманов Артур (директор департамента международной информационной безопасности) представил стратегию масштабирования международных киберучений под эгидой ООН.**
- **НКЦКИ – Анатолий Грачев сформулировал уроки учений ОДКБ+ и требования к национальным CERT.**

Промышленность и КИИ-операторы

- **Госкорпорация «Росатом» – Королев Андрей рассказал о платформе РБПО, центрах безопасной разработки и системе добровольной сертификации KIE Cert для радиоэлектронной продукции. Плановый срок перехода на российское ПО – до 2030 года.**
- **ПАО «ТМК» – Якоб Дмитрий поделился опытом двухнедельных DR-учений и описал SOC, фиксирующий несколько тысяч атак в месяц.**
- **АО «ТВЭЛ» – Гаранин Евгений представил данные о структуре бюджета ИБ (80/20) и росте стоимости ИТ-проектов на 30% из-за требований регуляторов.**
- **ПАО «ГМК «Норильский никель»» – Мартынцев Алексей рассказал о security data lake для прогнозирования атак на АСУ ТП и платформе БИБ-клуб (~100 компаний).**
- **ПАО «Аэрофлот» – Попов Денис подтвердил опыт реального инцидента и усиление SOC через AFLT Systems.**
- **Северсталь – Гусев Сергей назвал независимые red team проверки основным инструментом реальной оценки защищённости.**

Специализированные игроки ИБ

- **Positive Technologies – Новиков Алексей представил данные исследования по угрозам в промышленности и стратегию «измеряй и опережай».**
- **ИНФОСИСТЕМЫ ДЖЕТ – Елисеев Владимир привёл статистику проникновений через подрядчиков и модерировал ключевую сессию по непрерывности бизнеса.**

- **ГК «Солар» – Ефимов Антон отметил, что никто в России пока не знает, как строить доверенную ИИ-безопасность.**
- **Гарда – Хайретдинов Рустэм описал барьер взаимного недоверия на рынке киберстрахования.**
- **ООО «УЦСБ» – Богданов Валентин дал оценки рынка киберстрахования и типичных ошибок при построении защиты.**
- **ГК Инфовотч – Арефьев Андрей предложил связать страховые ставки со статусом импортозамещения.**

Финансовый сектор и страхование

- **ТБанк – Гадарь Дмитрий (CISO) представил концепцию machine-speed защиты, систему Nula и программу кибериспытаний.**
- **Страховой Дом ВСК – Фролов Роман раскрыл детали инцидента ноября 2025 года и ввёл термин «киберустойчивость» в деловой оборот.**
- **АО АльфаСтрахование – Скворцов Владимир и Буза Алексей описали два реальных страховых случая и статистику атак на КИИ.**
- **АО ГК «МЕДСИ» – Соколов Андрей сформулировал принцип Security by Design в медицинском секторе.**
- **АО «СОГАЗ» – Старостин Георгий представил модель бюджетирования через математическое ожидание ущерба.**
- **РК Страховой Брокер – Еремеев Иван привёл наиболее подробную статистику урегулированных киберстраховых случаев в России.**

Рынок M&A и инвестиции

- **Sk Capital – Попов Егор оценил инвестиционный потенциал российского рынка и структуру сделок.**
- **Группа компаний SolidLab – Железняков Вячеслав описал СП с «Яндексом».**
- **CICADA8 – Кузнецов Алексей представил стратегию монопродуктового роста в нише deception.**
- **CyberED – Богомолов Егор рассказал об экспортной программе обучения при поддержке Cyberus.**
- **АО Кибердом – Шадюк Александра сопоставила мировые инвестиционные тренды с российским рынком.**

Облачные и технологические компании

- **CLOUD.RU – Волков Сергей (CISO) описал уровень роботизации SOC (20%) и архитектурную изоляцию AI Factory.**
- **MTC WEB SERVICES – Бобыльков Виктор поставил под сомнение текущую пользу ИИ для ИБ и привёл данные о закрытых уязвимостях (97%).**

- **СберТех – Соленик Всеслав описал перевод 100+ систем в architecture as a code.**

11. Цитаты-якоря

Опорные высказывания спикеров ЦИПР-2026 по теме.

Угрозы и природа атак

> *«Из вашего бизнеса читают всю вашу переписку, знают, что вы будете делать, знают ваши переговорные позиции на ближайших, там, партнерских раундах и так далее. И вы просто теряете с точки зрения бизнеса эти деньги незаметно. И это печально.»*
>
> **Новиков Алексей, Управляющий директор, Positive Technologies**

> *«По нашей статистике, около половины всех случаев заход через подрядчиков. По крайней мере, для крупных организаций, гораздо легче взломать или проникнуть в инфраструктуру, доступ подрядчика, чем напрямую идти в большую организацию.»*
>
> **Елисеев Владимир, Генеральный директор, ИНФОСИСТЕМЫ ДЖЕТ**

> *«А мы прогнозируем, что к двадцать седьмому году это будут минуты. То есть мы не успеваем, от появления уязвимости, там, если вы ставите патч через три дня, то это у вас, скорее всего, уже будет поздно.»*
>
> **Гадарь Дмитрий, CISO, ТБанк**

Парадигма устойчивости

> *«риск взлома актуален для любой организации. И здесь вопрос не если, а вопрос когда, да? И вот мне сейчас нравится очень термин, да, не киберзащита, а киберустойчивость, которая, наверное, характеризуется, а как быстро компания может восстановиться после той кибератаки, которая произойдет.»*
>
> **Фролов Роман, Член совета директоров, Заместитель Генерального директора, Страховой Дом ВСК**

> *«Защита никогда не сможет обеспечить стопроцентную гарантию, что ни одна атака не пройдет. Но защита должна быть готова к тому, чтобы устранить последствия атак.»*
>
> **Хасин Евгений, Врио директора Департамента обеспечения кибербезопасности, Министерство цифрового развития, связи**

> *«от медведя не надо убегать первым. Вот в кибербезопасности не надо быть самым защищенным, надо быть защищеннее, чем сосед. И просто необходимо измерять, какой у вас уровень киберзащищенности, там, на- По отрасли, по сегменту и так далее.»*
>
> **Новиков Алексей, Управляющий директор, Positive Technologies**

Реальные инциденты и цена бездействия

> *«Буквально за день до того, как у нас это все произошло, мы сидели на правлении, обсуждали, а надо ли потратить на кибербез дополнительные сто миллионов рублей, да? И понятно, что все члены правления сказали: «Ну ты что? Сто миллионов рублей? Ты с ума сошел? Это вообще просто нереально». Вот. А в это время уже кто-то был внутри нас.»*
>
> **Фролов Роман, Член совета директоров, Заместитель Генерального директора, Страховой Дом ВСК**

> *«Раньше мы жили «сначала построим, а потом будем защищать». Сейчас уже это невозможно. Время сжато стало. Время не прощает. Любой человек с использованием искусственного интеллекта становится потенциальным хакером, и мы как бы с этим уже живем.»*
>
> **Соколов Андрей, Президент, АО ГК «МЕДСИ»**

> *«Еще раз вам повторяю семьдесят дней каждый день больше тысячи кибератак, но не было успешно ничего.»*
>
> **Джавади Мехди (через переводчика), цифровой банк Парсиан (Иран)**

ИИ, кооперация и рынок

> *«Nula, наша разработка, – это группа агентов, которая довольно эффективно встраивается в процессы информационной безопасности. Это атакующие агенты, которые в автономном режиме взламывают наши системы нон-стопом двадцать четыре на семь, не устают и делают за пятнадцать-двадцать минут то, что у топовых инженеров занимает двое-трое суток.»*
>
> **Гадарь Дмитрий, CISO, ТБанк**

> *«Я не вижу, что информационная безопасность – это область конкуренции компаний.»*
>
> **Гадарь Дмитрий, CISO, ТБанк**

> *«объем премий по киберстрахованию, которые собираются в России, вот не коробок каких-то, вот реального страхования, меньше миллиарда рублей, да? Что такое миллиард рублей? Это меньше одной тысячной от страхового рынка России.»*
>
> **Фролов Роман, Член совета директоров, Заместитель Генерального директора, Страховой Дом ВСК**

> *«компьютерные атаки – да, это всегда плохо, но еще хуже, когда уполномоченные организации двух стран, национальные CERT, не могут договориться, как нейтрализовать источник компьютерной атаки.»*
>
> **Анатолий Грачев (НКЦКИ)**

12. Сводная таблица ключевых метрик ЦИПР-2026

Числовые показатели темы, прозвучавшие в выступлениях на ЦИПР-2026. Все значения приведены строго по материалам сессий.

Показатель	Значение	Источник
Доля атак, приходящихся на объекты КИИ	**>75%**	Скворцов Владимир, АО АльфаСтрахование
Доля инцидентов в промышленности с применением вредоносного ПО	**80+ %**	Новиков Алексей, Positive Technologies

Показатель	Значение	Источник
Доля инцидентов в промышленности, вызывающих остановку бизнес-процессов	~1/3	Новиков Алексей, Positive Technologies
Стоимость аренды undetectable malware	$400	Новиков Алексей, Positive Technologies
Time to exploit к 2027 году	минуты	Гадарь Дмитрий, ТБанк
Страховая выплата АльфаСтрахование (шифрование промышленной компании)	10 млн руб.	Скворцов Владимир, АО АльфаСтрахование
Страховая выплата АльфаСтрахование (атака на добывающую компанию)	>100 млн руб.	Скворцов Владимир, АО АльфаСтрахование
Число урегулированных страховых случаев в России за 2 года	8 страховых случаев	Еремеев Иван, РК Страховой Брокер
Крупнейшая страховая выплата по киберинциденту в России	свыше 200 млн руб.	Еремеев Иван, РК Страховой Брокер
Объём реального корпоративного киберстрахования в России	менее 1 млрд руб.	Фролов Роман, Страховой Дом ВСК
Прогноз рынка киберстрахования в России к 2027–2028 году	10 млрд руб.	Богданов Валентин, ООО «УЦСБ»
Мировой рынок киберстрахования в 2024 году	14–15 млрд долл.	Богданов Валентин, ООО «УЦСБ»
Прогноз мирового рынка киберстрахования к 2028 году	более 100 млрд долл.	Богданов Валентин, ООО «УЦСБ»
Доля проникновений в крупных организациях через подрядчиков	>50%	Елисеев Владимир, ИНФОСИСТЕМЫ ДЖЕТ
Время восстановления ВСК после кибератаки	3 недели	Фролов Роман, Страховой Дом ВСК
Соотношение бюджета ИБ ТВЭЛ: предотвращение / восстановление	80/20	Гаранин Евгений, АО «ТВЭЛ»
Выполнение задачи агентом Nula vs. топовые инженеры	15–20 минут vs. 2–3 суток	Гадарь Дмитрий, ТБанк
Участники платформы БИБ-клуб (промышленная кооперация в ИБ)	~100 компаний	Мартынцев Алексей, ПАО «ГМК «Норильский никель»»

По материалам деловой программы ЦИПР-2026 (cipr.ru · platforms.su). Все цифры и формулировки приведены строго по выступлениям спикеров.