ЦИФРОВОЙ МАРКЕТПЛЕЙС

ПМЭФ-2026 · АНАЛИТИКА

Кибербезопасность и киберустойчивость КИИ

Угрозы, реагирование, страхование, ИИ-агенты и международная кооперация

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

Подготовлено АНО «Цифровые платформы»
ПМЭФ-2026 · Санкт-Петербург · 18–21 июня 2026
diplatforms.ru · platforms.su

Оглавление

По материалам деловой программы ПМЭФ-2026. Все цифры и формулировки приведены строго по выступлениям спикеров. Подготовлено АНО «Цифровые платформы».

Кибербезопасность и киберустойчивость КИИ

> *ПМЭФ-2026 зафиксировал смену повестки в кибербезопасности: от технической гигиены к системной киберустойчивости — способности функционировать под непрерывным огнём. Четыре ключевых сессии форума дали исчерпывающий срез угроз для КИИ, новой парадигмы реагирования, угрозы дипфейков и вопросов финансовой ответственности за инциденты.*

1. Краткое резюме и ключевые выводы

1. **Каждая пятая российская компания взломана и не знает об этом.** По собственной оценке BI.ZONE, большинство организаций обнаруживают проникновение лишь спустя месяцы; типовая картина — преступники находятся в инфраструктуре жертвы более полугода, а иногда годами. Это означает, что стандартные меры обнаружения угроз системно не работают. (Самарцев Дмитрий, BI.ZONE)
2. **Средний финансовый ущерб от успешной кибератаки — не менее 50 миллионов рублей.** В резонансных случаях потери значительно выше: Страховой Дом ВСК потерял порядка 900 миллионов рублей по марже в результате атаки 12 ноября, при этом злоумышленники запросили выкуп в размере около 1 миллиарда рублей. (Самарцев Дмитрий, BI.ZONE; Цикалюк Сергей, ВСК)
3. **Более 40% кибератак преследуют цели шпионажа и кражи информации.** Тройка главных целей как криминальных, так и государственно-мотивированных злоумышленников — государственные органы, финансовые организации и логистика. За большинством взломов стоят не деструктивные, а разведывательные задачи. (Самарцев Дмитрий, BI.ZONE)
4. **Количество кибератак с применением ИИ выросло более чем на 90% за 2025 год.** ИИ-агенты уже сегодня автономно атакуют инфраструктуру — компании этого не видят. Злоумышленники претендуют на лидерство в применении ИИ, опережая защитников; применение ИИ повысит возможности атакующих не на порядок, а на два в течение ближайшего полугода-года. (Самарцев Дмитрий, BI.ZONE; Кузнецов Станислав, Сбербанк; Симис Борис, Positive Technologies)
5. **54% поднадзорных ФСТЭК организаций имеют критические уязвимости на сетевом периметре.** 69% не используют двухфакторную аутентификацию для привилегированных пользователей, около 42% эксплуатируют пароли по умолчанию. В ходе работы с организациями приграничных территорий ФСТЭК обнаружила 29 000 IP-адресов, о существовании которых организации не подозревали. (Лютиков Виталий, ФСТЭК России)
6. **Основной вектор крупных инцидентов — проникновение через подрядную организацию.** ВСК атаковали через аудиторскую компанию-партнёра; анализ последних крупных инцидентов показывает, что в большинстве случаев злоумышленники заходят именно через подрядчиков — этот вектор систематически недооценивается службами безопасности. (Лютиков Виталий, ФСТЭК России; Цикалюк Сергей, ВСК)
7. **Рост числа дипфейков за полтора года — в 26 раз; ущерб превысил 2 миллиарда рублей.** Создание дипфейка стоит не более 50 рублей, тогда как средний чек хищения при его применении составляет 16 миллионов рублей с одной атаки. В теневом интернете доступно более 40 000 готовых дипфейк-заготовок. К концу 2026 года потери от этого вида преступлений могут составить 250 миллиардов рублей. (Кузнецов Станислав, Сбербанк)

8 **Ущерб от кибермошенничества в 2025 году — 195 миллиардов рублей; вернуть удалось лишь 1%.** Вместе с тем наметился перелом: число мошеннических атак снизилось с 9 до 6 тысяч в неделю, общий объём киберпреступлений сократился на 11,8%. Создана антифрод-платформа, объединившая банки, операторов связи и государство. (Скабеева Ольга, Россия 1; Храпов Андрей, МВД; Григоренко Дмитрий, Правительство РФ)

9 **Атаки на предприятия ОПК выросли в 7 раз; цифровизация сформировала новые векторы атак на КИИ.** Системы управления теплоснабжением, водоснабжением и котельными в реальном времени, электроэнергетика без цифровой инфраструктуры не функционирует. Атака на цифровые системы управления энергосетью приводит к немедленным физическим последствиям. (Опадчий Фёдор, СО ЕЭС; Ересько Алексей, Минстрой; Николаев Айсен, Республика Саха)

10 **Регуляторная модель фактически наказывает компании за публичную открытость об инцидентах.** На ПМЭФ-2026 крупная частная компания впервые открыто признала факт взлома — рассказала, как происходила атака, какой ущерб был нанесён и какие ошибки допущены. Это исключение из правил, а не норма. Существующий подход стимулирует скрывать инциденты. (Кузнецов Станислав, Сбербанк)

11 **Российская система защиты от кибермошенничества признана одной из лучших в мире.** Многие страны берут на вооружение российские решения; финтех и телеком России — одни из самых продвинутых в мире по инструментам блокировки мошенников. Объединённая система имеет высокий экспортный потенциал. (Храпов Андрей, МВД; Галактионова Инесса, МТС; Касперский Евгений, Лаборатория Касперского)

12 **Для системной защиты необходим «цифровой иммунитет» — минимальный набор требований для всего цифрового пространства страны.** Предложено создать координационный штаб под руководством Григоренко с технической рабочей группой, имеющей право доклада наверх. Создание единого органа по кибербезопасности остаётся нерешённой задачей из-за межведомственных противоречий. (Кузнецов Станислав, Сбербанк)

2. Контуры темы: сессии и повестка

2.1 «Стресс-тест в реальном времени: как не потерять миллиарды при кибератаке» (сессия 157236)

Центральная сессия ПМЭФ-2026 по кибербезопасности объединила первых лиц пострадавших компаний, регуляторов и ведущих вендоров. Впервые в российской практике крупная частная компания — Страховой Дом ВСК — публично и детально рассказала об атаке, которую пережила 12 ноября: отключение связи, блокировка ПО, потеря доступа к клиентским данным и требование выкупа в размере около 1 миллиарда рублей.

Участники сессии: Дмитрий Самарцев (BI.ZONE), Сергей Цикалюк (ВСК), Виталий Лютиков (ФСТЭК России), Станислав Кузнецов (Сбербанк). Модерация — РБК. Ключевые тезисы: масштаб проблемы неуправляемой поверхности атаки, провал культуры раскрытия инцидентов, дефицит профессиональных переговорщиков с вымогателями, предложение концепции «цифрового иммунитета».

2.2 «Цифровая устойчивость экономики в эпоху глобальных киберконфликтов» (сессия 156679)

Сессия рассматривала кибербезопасность как вопрос национальной и экономической устойчивости в условиях продолжающегося геополитического противостояния. Борис Симис (Positive Technologies) обозначил культурный и управленческий разрыв: информационную безопасность нельзя построить без прямого участия первого лица компании.

Виталий Лютиков (ФСТЭК) представил кейс Якутии: 10 суток DDoS-атаки с более чем 1400 эпизодами в мае, ответом на которую стало создание Центра противодействия киберугрозам 24/7 в ноябре 2024 года. Антон Горелкин (Госдума) описал наступательную киберстратегию США и коммерциализацию DDoS-атак как услуги по подписке. Виктор Евтухов (Управление Президента) предупредил о полной автоматизации управления КИИ и её последствиях для кибербезопасности.

2.3 «Цифровой самозванец: новое оружие массового поражения» (сессия 157239)

Сессия была посвящена дипфейкам как системной угрозе — не только для частных лиц, но и для политической стабильности, деловой жизни и выборного процесса. Станислав Кузнецов (Сбербанк) представил три поколения дипфейков: «кружочек» (короткое видео), «фейк-маска» (маскировка в видеозвонке) и «фейк-аватар» (полностью цифровой собеседник с ИИ-интеллектом).

В ходе сессии был продемонстрирован антидот — проект «Алитея»: сервис на основе ИИ, способный за короткое время определить, является ли видео дипфейком. Данил Филиппов (МВД) сообщил, что за четыре месяца зафиксировано 90 тысяч мошенничеств, из них около 4% с применением дипфейков. Прогноз по распространению дипфейков на русскоязычную и затем глобальную аудиторию с учётом мультиязычных аватаров — до 8 миллиардов потенциальных жертв.

2.4 «Кибермошенничество: кому платить по счетам?» (сессия 161858)

Ключевая дискуссионная сессия с участием вице-премьера Дмитрия Григоренко, Андрея Храпова (МВД), Инессы Галактионовой (МТС) и Евгения Касперского. Повестка — распределение финансовой ответственности за ущерб от кибермошенничества между гражданином, банком и оператором связи.

МВД констатировало первый перелом в статистике: общий объём мошенничеств сократился на 11,8%, число пострадавших — на 5,5%. В центре дискуссии — антифрод-платформа, объединившая всех участников рынка, и вопрос: достаточно ли технических мер или мошенничество как «злоупотребление доверием» требует принципиально иных подходов.

2.5 «Международная кооперация: технологии без людей, как люди без технологий» (сессия 156761)

Юрий Максимов (Positive Technologies) представил концепцию помощи дружественным странам в создании суверенных компаний и отраслей кибербезопасности по российским лекалам. Акцент — не на продаже продуктов, а на передаче компетенций: через четыре года у страны появляется своя компания, через пять — своя индустрия.

Обсуждалась и тема кибериспытаний как международного инструмента кооперации: совместные хакерские соревнования между дружественными странами формируют доверие и практическое взаимодействие лучше, чем любые договоры.

2.6 «Цифровое будущее: общие векторы развития, вызовы и решения» (сессия 156764)

Международная сессия с участием представителей Казахстана, Беларуси, Узбекистана и Таджикистана, посвящённая гармонизации подходов к кибербезопасности в пространстве СНГ. Кирилл Залесский (Нацбанк Беларуси) представил опыт автоматизированной системы обработки инцидентов, позволяющей реагировать в течение десятков минут.

Исфандиёри Саъдулло (Таджикистан) предложил создать в рамках РСС единую платформу мониторинга киберугроз для всех стран региона. Участники констатировали: кибермошенничество носит выраженный трансграничный характер — решить проблему в одной стране без координации с соседями невозможно.

3. Промышленность под ударом: угрозы и векторы атак

3.1 Масштаб и характер угроз

По оценке BI.ZONE, каждая пятая российская компания взломана и не знает об этом — обнаружение проникновения происходит лишь спустя месяцы. Типовая картина: злоумышленники находятся внутри инфраструктуры более полугода, а нередко годами, прежде чем будут обнаружены или перейдут к активной фазе атаки.

Тройка главных целей — государственные органы, финансовые организации и логистика. Более 40% атак преследуют цели шпионажа и добычи информации, что означает: за большинством взломов стоит не деструкция, а разведывательные задачи. Количество атак на предприятия оборонно-промышленного комплекса выросло в 7 раз (Опадчий Фёдор, СО ЕЭС).

> *«По собственной оценке BI.ZONE, каждая пятая российская компания взломана и не знает об этом. Это системная проблема: большинство организаций обнаруживают проникновение лишь спустя месяцы.»*
>
> *(Самарцев Дмитрий, BI.ZONE)*

3.2 КИИ под огнём: энергетика, ЖКХ, медицина

Современная электроэнергетика без цифровой инфраструктуры не функционирует: управление энергосистемой, диспетчеризация, балансировка нагрузок — всё это цифровые процессы. Атака на системы управления энергосетью приводит к немедленным физическим последствиям: отключению потребителей, разбалансировке системы, каскадным авариям. Время реакции — секунды (Николаев Айсен, Республика Саха).

В ЖКХ ситуация принципиально сложнее, чем в электроэнергетике: 11 000 ресурсоснабжающих организаций с разрозненными системами теплоснабжения и водоснабжения — единого системного оператора нет. Минстрой прорабатывает создание двух центров кибербезопасности: ведомственного и отраслевого на базе Дом.РФ (Ересько Алексей, Минстрой).

Медицина является особо чувствительной отраслью: взлом медицинских систем — это не просто утечка данных, но и разведка состояния здоровья политических деятелей, шантаж, а в крайних случаях — деструктивное воздействие на оборудование жизнеобеспечения. ФМБА совместно с Positive Technologies строит отраслевой центр безопасности здравоохранения (Лишин Николай, ФМБА).

> *«Применение цифровых технологий без элементов кибербезопасности — всё равно что кушать грязными руками. Скорость цифровизации ЖКХ без синхронной защиты создаёт риски не для отдельных компаний, а для всего населения страны.»*
>
> *(Ересько Алексей, Минстрой)*

3.3 Унаследованное иностранное оборудование как критическая уязвимость

Межсетевой экран Fortigate получил 120 задокументированных уязвимостей за последний год, из которых около 10% активно эксплуатируются в реальных атаках. При этом обновить устройство невозможно: доступ к легальным обновлениям закрыт, поддержка прекращена. Аналогичная ситуация — с оборудованием Cisco.

Вендоры программного обеспечения намеренно оставляют уязвимости незакрытыми — в интересах спецслужб страны происхождения. Это означает, что импортное ПО на критической инфраструктуре — не просто технический риск, а стратегическая угроза (Горелкин Антон, Госдума).

> *«Организации по всей стране продолжают использовать унаследованные решения Fortinet и Cisco, хотя поддержка и доступ к обновлениям для них закрыты. Обновить оборудование невозможно, а уязвимости в нём активно эксплуатируются — это фундаментальный барьер для защиты инфраструктуры.»*
>
> *(Лютиков Виталий, ФСТЭК России)*

3.4 Цепочки поставок и подрядчики как вектор входа

Анализ последних крупных инцидентов показывает: в большинстве случаев злоумышленники заходят в инфраструктуру жертвы через подрядные организации. Именно так была атакована ВСК — через доверенную аудиторскую компанию-партнёра. После инцидента ВСК сменила аудитора.

Для малого и среднего бизнеса кибербезопасность не входит в стратегические приоритеты. Но когда малый бизнес становится частью цепочки поставок крупного предприятия, его уязвимость становится уязвимостью всей системы (Симис Борис, Positive Technologies). Атака на Jaguar Land Rover привела к остановке производства у около 5 000 подрядчиков — аналогичные риски актуальны для российской промышленности (Касперский Евгений, Лаборатория Касперского).

> *«Вектором входа в инфраструктуру ВСК оказалась аудиторская компания, с которой компания работала. Преступники зашли через доверенного подрядчика — после инцидента ВСК сменила аудитора.»*
>
> *(Цикалюк Сергей, Страховой Дом ВСК)*

3.5 Поверхность атаки: неуправляемый периметр

В ходе работы с организациями приграничных территорий ФСТЭК обнаружила 29 000 IP-адресов, которые организации не использовали и не знали об их существовании. Все они были заблокированы без каких-либо последствий — это наглядно демонстрирует масштаб неуправляемой поверхности

атаки.

По мере развития цифровизации все аналоговые резервные процессы деградируют: их забывают, никто не поддерживает. При кибератаке компании обнаруживают, что альтернативы отключённым сервисам нет. Критически важные процессы необходимо сохранять в аналоговом виде и периодически проверять их работоспособность (Лютиков Виталий, ФСТЭК).

> *«По данным мониторинга ФСТЭК, в пятидесяти четырёх процентах организаций на сетевом периметре сохраняются известные критические уязвимости. Шестьдесят девять процентов не используют двухфакторную аутентификацию для привилегированных пользователей, а около сорока двух процентов эксплуатируют пароли по умолчанию.»*
>
> *(Лютиков Виталий, ФСТЭК России)*

4. От киберзащиты к киберустойчивости: смена парадигмы

4.1 Новая парадигма: функционировать под огнём

Центральный сдвиг, зафиксированный на ПМЭФ-2026: от логики «защитить периметр, не пустить врага» к логике «обеспечить устойчивое функционирование в условиях постоянных успешных атак». Многие компании не взломаны не потому, что хорошо защищены, а потому что до них ещё не дошли руки достаточно квалифицированного злоумышленника (Симис Борис, Positive Technologies).

Кибербезопасность нужно воспринимать как регулярный медицинский чекап, а не как скорую помощь. Компания, которая проверяет свою защищённость раз в год, находится в принципиально иной позиции, чем та, которая реагирует только после инцидента. Кибериспытания — регулярная проверка реальной защищённости путём контролируемых атак — стали нормой для передовых компаний.

> *«Многие компании не взломаны не потому, что хорошо защищены, а потому что до них ещё не дошли руки достаточно квалифицированного злоумышленника. Наш масштаб пока спасает — но с массовым применением ИИ атакующими это преимущество исчезнет в течение полугода-года.»*
>
> *(Симис Борис, Positive Technologies)*

4.2 Культурный и управленческий разрыв

Информационная безопасность не может быть делегирована ИТ-службе — её нельзя построить без прямого участия первого лица компании. Пока руководитель воспринимает кибербезопасность как технический вопрос, стратегической защиты нет (Симис Борис, Positive Technologies).

Уровень знаний руководителей организаций в области ИБ и кибергигиены находится ниже элементарного. Это означает, что даже при наличии инцидента лица, принимающие решения, не понимают, что должны делать. Реальный кейс: руководитель ФОИВ, узнав о взломе 500 компьютеров ведомства, запретил кому-либо об этом сообщать (Кузнецов Станислав, Сбербанк).

> *«Кибербезопасность — это прежде всего культурный процесс. Технологии — необходимое, но не достаточное условие. Организация, в которой каждый сотрудник понимает свою роль в защите данных, защищена принципиально лучше, чем та, где установлен самый дорогой файрволл, но нет культуры.»*
>
> *(Симис Борис, Positive Technologies)*

4.3 Концепция «цифрового иммунитета»

Для системной защиты необходимо ввести понятие цифрового иммунитета: минимальный набор требований, определяемый регуляторами и хеджирующий любые киберриски. В него должны входить правила поведения при инциденте и обязательные процессы, внедрённые фактически на всём цифровом пространстве страны (Кузнецов Станислав, Сбербанк).

Аналогия с пандемией предложена МВД: как общество справилось с ковидом через создание общего иммунитета — цифровые «киберпрививки» необходимо устанавливать как общую вакцину. Кибербезопасность должна стать столь же привычной, как мытьё рук (Лишин Николай, ФМБА; Филиппов Данил, МВД).

> *«Для системной защиты необходимо ввести понятие цифрового иммунитета: минимальный набор требований, определяемый регуляторами и хеджирующий любые киберриски. В него должны входить правила поведения при инциденте и обязательные процессы, внедрённые фактически на всём цифровом пространстве страны.»*
>
> *(Кузнецов Станислав, ПАО Сбербанк)*

4.4 Зонтичная защита и отраслевые центры

Для предприятий ОПК разработана модель зонтичной защиты: единый периметр кибербезопасности охватывает множество предприятий, а не каждое строит защиту самостоятельно. Это позволяет концентрировать экспертизу и снижать нагрузку на небольшие предприятия (Опадчий Фёдор, СО ЕЭС).

Системный оператор Единой энергосистемы разработал семь принципов кибербезопасности для объектов электроэнергетики, охватывающих весь цикл от проектирования систем управления до реагирования на инциденты. Одна из главных нерешённых задач — жёсткая сегментация систем оперативно-диспетчерского управления и корпоративных сетей (Николаев Айсен, Республика Саха).

Минстрой прорабатывает создание ведомственного центра кибербезопасности и отраслевого Центра на базе Дом.РФ. ФМБА совместно с Positive Technologies строит отраслевой центр безопасности для здравоохранения.

4.5 Открытость об инцидентах как системный вопрос

Существующая регуляторная модель фактически наказывает компании за публичную открытость о взломах и стимулирует скрывать инциденты. Это системная проблема, которая мешает обмену информацией и развитию отраслевой защиты. Большинство организаций предпочитают скрывать инциденты — что препятствует развитию отраслевой культуры кибербезопасности (Кузнецов Станислав, Сбербанк).

Публичное признание факта атаки ВСК на ПМЭФ стало историческим прецедентом: на одном из главных деловых форумов страны крупнейшая частная компания впервые открыто рассказала, как

именно происходила атака, какой ущерб был нанесён и как следует избегать подобных ошибок.

> *«Существующая регуляторная модель в области информационной безопасности фактически наказывает компании за публичную открытость о взломах и стимулирует скрывать инциденты. Это системная проблема, которая мешает обмену информацией и развитию отраслевой защиты.»*
>
> *(Кузнецов Станислав, ПАО Сбербанк)*

5. Кибермошенничество и дипфейки: новое оружие

5.1 Взрывной рост дипфейков: масштаб и экономика угрозы

За полтора года рост числа дипфейков в России составил 26 раз. В теневом интернете доступно более 40 000 готовых заготовок — их приобретение и использование не требует специальных знаний или навыков ИТ-специалиста. Создание одного дипфейка обходится не более чем в 50 рублей, тогда как средний чек хищения при его применении составляет 16 миллионов рублей с одной атаки.

Ущерб от дипфейков уже превысил 2 миллиарда рублей; по прогнозу Сбербанка, к концу 2026 года потери от этого вида преступлений в России могут составить 250 миллиардов рублей. По данным Интерпола, маржинальность дистанционных мошенничеств в 4 раза выше, чем традиционных.

> *«За полтора года, может быть даже чуть меньше, произошёл колоссальный рост дипфейков в нашей стране. Они исчисляются не в проценты, не в разы, а уже в двадцать шесть раз.»*
>
> *(Кузнецов Станислав, ПАО Сбербанк)*

> *«Станислав Константинович, нас ждёт взрывной рост мошенничества с использованием deepfake. Только от этого вида преступлений Россия может потерять двести пятьдесят миллиардов рублей к концу этого года.»*
>
> *(Анастасия, проект «Алитея», Сбербанк)*

5.2 Три поколения дипфейков и эволюция мошеннических схем

Сбербанк описал три поколения дипфейков: «кружочек» — короткое синтетическое видео для мессенджеров; «фейк-маска» — наложение маски на реального человека в видеозвонке в реальном времени; «фейк-аватар» — полностью цифровой собеседник, использующий знания ИИ и способный вести диалог.

Сценарии мошенничества принципиально изменились: они становятся длительными (дни, недели, иногда месяцы), работая глубоко с жертвой и медленно доводя её до принятия решения о передаче денег. Мошенники взламывают Telegram-аккаунты, изучают переписки и контакты, после чего ведут целевые, высококонтекстные атаки — что делает обман значительно более убедительным.

> *«Голос близкого человека становится командой, лицо руководителя — пропуском. Новость от авторитетного источника — триггером для управления сотнями тысяч людей. Главная атака происходит не на устройство, она происходит внутри решения поверить, нажать, подтвердить, переслать.»*
>
> *(Нарратор видеоролика, Сбербанк)*

5.3 Угроза для политики и государственного управления

Дипфейки угрожают не только гражданам — они способны дискредитировать политиков накануне выборов, влиять на решения советов директоров и провоцировать военные конфликты. Волна дипфейков депутатов и сенаторов ожидается к сентябрю в преддверии выборов (Жданов Юрий, КС генпрокуроров СНГ).

Дипфейк — технология, подрывающая доверие: граждан к государству, к экономике. Мультиязычные аватары способны расширить аудиторию мошенников с 258 миллионов до 8 миллиардов человек — с любого языка на любой в режиме реального времени (Шейкин Артём, Совет Федерации; Филиппов Данил, МВД).

> *«Дипфейк — это технология, которая подрывает доверие, подрывает доверие граждан, государству, к экономике.»*
>
> *(Шейкин Артём, Совет Федерации)*

5.4 Технологические ответы: «Алитея» и МТС Защитник

Сбербанк представил проект «Алитея» — сервис на основе ИИ для распознавания дипфейков в видеофайлах. Любое видео может быть подвергнуто экспертизе в короткое время, после чего система выдаёт заключение: фейк или подлинник. В ходе сессии была продемонстрирована работа сервиса в прямом эфире.

МТС Защитник в начале 2026 года научился обнаруживать видеодипфейки за 3 секунды — технология определяет, что голос или видеоизображение собеседника подменены. По аналитике МТС, число мошеннических звонков снизилось на 40%, хотя сами звонки становятся сложнее: мошенники активно используют ИИ и дипфейки голоса и видео.

> *«Мы можем найти так называемую серебряную пулю очень быстро, потому что такого рода технологии, сложные технологии должны побеждать тоже технологии.»*
>
> *(Кузнецов Станислав, ПАО Сбербанк)*

5.5 Правовое регулирование и защита цифровой личности

МВД предложило законодательно защитить «цифровую личность» — так же, как физическую, через соответствующие нормы УК и КоАП. В настоящее время правоохранительные органы не готовы к волне дипфейков: специалистов по цифровым преступлениям катастрофически мало.

Общество не понимает, в каких областях будут использоваться дипфейки. Даже эксперты по кибербезопасности сами распространяют непроверенные фейки, не замечая этого. Главная задача — развитие критического мышления и цифровой грамотности населения (Шейкин Артём, Совет

Федерации; Жданов Юрий, КС генпрокуроров СНГ).

6. Реальные инциденты: кейсы и уроки

6.1 Кейс ВСК: атака 12 ноября и её анатомия

12 ноября в ВСК произошёл масштабный инцидент: перестала работать телефонная связь, заблокировалось ПО, был полностью закрыт доступ к клиентской информации и взаиморасчётам с банками, лизинговыми компаниями и медицинскими учреждениями. Реальные потери компании составили порядка 900 миллионов рублей по марже — не считая репутационных потерь и затрат на восстановление.

Злоумышленники запросили выкуп около 1 миллиарда рублей. Вектором входа оказалась аудиторская компания-партнёр. ВСК привлекла одного из немногих профессиональных переговорщиков в России; переговорщик с вероятностью более 90% определил, что у преступников нет базы данных — что впоследствии подтвердилось. В стране буквально единицы специалистов, способных вести такие переговоры профессионально.

> *«12 ноября прошлого года в ВСК произошёл масштабный инцидент, который руководство компании охарактеризовало как шок. Перестала работать телефонная связь — невозможно было позвонить даже внутри офиса. Именно тогда стала очевидна реальная цена недостаточных вложений в информационную безопасность.»*
>
> *(Цикалюк Сергей, Страховой Дом ВСК)*

6.2 DDoS на Якутию: 10 суток, 1400 эпизодов

В мае Республика Саха (Якутия) подверглась масштабной DDoS-атаке: 10 суток непрерывного воздействия, более 1400 отдельных эпизодов. Атака была направлена против цифровых сервисов, от которых зависит ежедневная жизнь населения. В условиях экстремального климата (−50°C) отключение систем теплоснабжения или связи — это прямая угроза жизни людей.

Ответом стало создание в ноябре 2024 года Центра противодействия киберугрозам с режимом мониторинга 24/7. В Северо-Восточном федеральном университете открыта кафедра кибербезопасности с первым набором в 26 студентов; колледж связи ежегодно выпускает более 60 специалистов (Лютиков Виталий, ФСТЭК; Николаев Айсен, Республика Саха).

> *«В Якутии цифровая инфраструктура — это не удобство, а вопрос выживания в экстремальном климате. При минус пятидесяти градусах отключение системы теплоснабжения или связи — это прямая угроза жизни людей.»*
>
> *(Лютиков Виталий, ФСТЭК России)*

6.3 Ликвидация «Гласа Бога» и торговля персональными данными

В январе 2025 года сотрудники полиции ликвидировали пробивочный сервис «Глас Бога». По оставшимся данным, только за январь было продано около миллиона персональных данных. В течение

2025 года из этого массива в отношении 15 000 граждан были совершены дистанционные мошенничества — общий ущерб составил 13 миллиардов рублей.

Ключевую роль в распространении кибермошенничества сыграло колоссальное количество незаконных персональных данных: именно они дают преступникам возможность набрать любой телефон, соединиться с человеком и дистанционно вывести деньги (Храпов Андрей, МВД).

> *«В январе 2025 года сотрудники полиции ликвидировали пробивочный сервис Глас Бога. По оставшимся данным только за январь было продано порядка миллиона персональных данных. В течение 2025 года из этого массива в отношении пятнадцати тысяч граждан были совершены дистанционные мошенничества — общий ущерб составил тринадцать миллиардов рублей.»*
>
> *(Храпов Андрей, МВД России)*

6.4 Взлом ФОИВ: 500 заражённых компьютеров и запрет на раскрытие

Показательный кейс, описанный на ПМЭФ: когда специалисты по безопасности сообщили руководителю федерального органа исполнительной власти о том, что хакеры находятся внутри инфраструктуры ведомства и заражены более 500 компьютеров, реакция последовала через 10 минут — звонком с вопросом «откуда вы узнали?» и прямым запретом кому-либо об этом сообщать.

Этот руководитель фактически дал преступникам возможность продолжать действовать. Кейс иллюстрирует одновременно две проблемы: критически низкий уровень компетенций топ-менеджмента в ИБ и отсутствие механизма, обязывающего сообщать об инцидентах (Кузнецов Станислав, Сбербанк).

> *«Когда специалисты по безопасности сообщили руководителю федерального органа исполнительной власти о том, что хакеры находятся внутри инфраструктуры ведомства и заражены более пятисот компьютеров, реакция последовала через десять минут. Звонок с вопросом: откуда вы узнали? После чего — прямой запрет кому-либо об этом сообщать.»*
>
> *(Кузнецов Станислав, ПАО Сбербанк)*

6.5 Фрагментация ГИС: системная проблема архитектуры

Системная проблема российской ИТ-архитектуры — фрагментация: каждое ведомство строит собственную государственную информационную систему. В результате вместо единой защищаемой инфраструктуры сотни изолированных систем с разными стандартами безопасности и многократно дублированными уязвимостями. Защищать это по-настоящему невозможно (Симис Борис, Positive Technologies).

В госсекторе средства выделяются на цифровизацию — и за неё спрашивают. За кибербезопасность не спрашивают. В результате уровень цифровизации растёт, а уровень защищённости — нет. Чем выше цифровизация, тем шире поверхность атаки и тем привлекательнее цель (Лишин Николай, ФМБА).

7. ИИ в арсенале атакующих и защитников

7.1 ИИ на стороне атакующих: качественный скачок

За 2025 год количество кибератак с применением инструментов ИИ возросло более чем на 90%. ИИ-агенты уже сегодня автономно осуществляют атаки на инфраструктуру — компании этого даже не видят. Это не сценарий будущего, это уже произошло (Кузнецов Станислав, Сбербанк).

Применение ИИ злоумышленниками в ближайшие полгода-год повысит их возможности не на порядок, а на два. Это качественный скачок: атаки, которые сегодня требуют команды профессионалов, станут доступны одному человеку с ноутбуком. Киберстратегия США сформулирована как наступательная; DDoS-атаки продаются по подписке на коммерческих платформах — порог входа в кибервойну снизился до уровня частного лица с кредитной картой (Симис Борис, Positive Technologies; Горелкин Антон, Госдума).

> *«Агенты на базе искусственного интеллекта уже сегодня автономно осуществляют атаки на инфраструктуру. Компании этого даже не видят. Это не сценарий будущего — это уже случилось. Отрасль в этом плане явно опаздывает.»*
>
> *(Кузнецов Станислав, ПАО Сбербанк)*

7.2 ИИ как инструмент защиты

Когда атаки автоматизированы с помощью ИИ, человек не успевает реагировать. Противодействовать ИИ может только ИИ — гонка вооружений в киберпространстве переходит в плоскость машинного времени: решения принимаются за миллисекунды (Евтухов Виктор, Управление Президента).

Лаборатория Касперского использует инструменты машинного обучения уже более 20 лет — ещё до появления термина «искусственный интеллект». ИИ значительно помогает в задачах анализа угроз, поиска аномалий и автоматизированного реагирования на инциденты (Касперский Евгений, Лаборатория Касперского).

Вместе с тем открыта уязвимость ИИ-систем защиты: их можно «накормить» подготовленными данными, вызвав галлюцинации — ложные срабатывания или пропуски угроз. Этот вектор атаки на сами системы ИБ пока не имеет проработанного ответа (Касперский Евгений, Лаборатория Касперского).

> *«Когда атаки автоматизированы с помощью искусственного интеллекта, человек не успевает реагировать. Противодействовать ИИ может только ИИ. Это означает, что гонка вооружений в киберпространстве переходит в плоскость машинного времени — решения принимаются за миллисекунды.»*
>
> *(Евтухов Виктор, Управление Президента РФ)*

7.3 ИИ и критическая инфраструктура: риск полной автоматизации

Движение к полной автоматизации управления КИИ неизбежно с точки зрения эффективности. Но это означает, что кибератака на автоматизированную систему имеет мгновенные физические последствия: отключение электричества, воды, тепла. Разрыв между скоростью цифровизации и зрелостью защиты нарастает.

Возможность создания ситуационного центра кибербезопасности для транспортных и роботизированных систем (Vehicle SOC) рассматривается в России — для централизованного выявления угроз перехвата управления и перепрошивки (Глущенко Вадим, Positive Technologies).

> *«Мы движемся к полной автоматизации управления критической информационной инфраструктурой. Это неизбежно с точки зрения эффективности. Но это означает, что кибератака на автоматизированную систему имеет мгновенные физические последствия — отключение электричества, воды, тепла.»*
>
> *(Евтухов Виктор, Управление Президента РФ)*

7.4 ИИ в мошенничестве: конец языкового барьера

Мультиязычные аватары в режиме реального времени переводят с любого языка на любой — это означает конец «языкового барьера» для мошенников. Если сейчас русские звонят русским, а китайцы — китайцам, то с распространением мультиязычных аватаров аудитория потенциальных жертв расширится до 8 миллиардов человек (Филиппов Данил, МВД).

Классические киберпреступники, пользуясь интересом к ИИ, активно распространяют вирусы под видом программ доступа к нейросетям. Только в 2026 году зафиксировано около 100 000 подобных случаев (Гербер Михаил, Лаборатория Касперского).

8. Кому платить по счетам: ответственность и страхование

8.1 Масштаб финансовых потерь и вопрос возмещения

По данным МВД, ущерб от кибермошенничества в 2025 году составил 195 миллиардов рублей. При этом вернуть гражданам удалось только 1,7 миллиарда — фактически около 1%. Средний финансовый ущерб от корпоративной кибератаки — не менее 50 миллионов рублей; потери ВСК составили около 900 миллионов рублей по марже.

Возмещение ущерба — не просто вопрос справедливости, а стимул для того, чтобы каждый участник рынка — банк, оператор, государство — совершал конкретные действия по борьбе с мошенничеством. Когда расплачивается только один участник, а остальные не несут последствий, эффективность системы принципиально иная (Григоренко Дмитрий, Правительство РФ).

> *«По данным МВД, в прошлом году ущерб от мошенников составил сто девяносто пять миллиардов рублей. При этом вернуть гражданам удалось только один миллиард семьсот миллионов — то есть фактически один процент.»*
>
> *(Скабеева Ольга, Телеканал «Россия 1»)*

8.2 Трёхстороннее распределение ответственности

В любом процессе кибермошенничества участвуют трое: сам гражданин, банк и оператор. У каждого — свои роли и зоны ответственности. Банк может заблокировать операцию, оператор — прервать сессию. Вопрос — какова доля ответственности каждого при причинении ущерба.

Если переложить ответственность за полную компенсацию на операторов связи или банки, возникнет новая волна мошенничества: люди будут снимать деньги сами, прятать их и заявлять о вымогательстве, требуя компенсацию — МВД захлестнёт поток таких дел. Системная проблема: единица звонка для мошенника стоит очень дёшево, а единица оперативных мероприятий на один звонок — очень дорого (Федулов Влад, Авито).

> *«Если переложить ответственность за полную компенсацию на операторов связи или банки, возникнет новая волна мошенничества: люди будут снимать деньги сами, прятать их и заявлять о вымогательстве, требуя компенсацию.»*
>
> *(Федулов Влад, Авито)*

8.3 Киберстрахование: от идеи к практике

Идея создания страхового продукта от кибератак обсуждалась в отрасли около 10 лет. Теперь, пережив атаку на собственную инфраструктуру, ВСК намерена разработать и предложить рынку страхование от киберрисков — этот вид страхования должен развиваться наравне с другими.

Рынок киберстрахования в России находится на начальном этапе: страховщики не имеют накопленной актуарной статистики, а сами компании нередко скрывают инциденты, что делает расчёт рисков крайне сложным. Открытость ВСК на ПМЭФ создаёт прецедент, который может изменить отношение рынка к публичному раскрытию (Цикалюк Сергей, ВСК).

> *«Идея создания страхового продукта от кибератак обсуждалась в отрасли около десяти лет. Теперь, пережив атаку на собственную инфраструктуру, ВСК намерена разработать и предложить рынку страхование от киберрисков.»*
>
> *(Цикалюк Сергей, Страховой Дом ВСК)*

8.4 Антифрод-платформа: успех кооперации

Создана антифрод-платформа — система, вынудившая всех участников рынка объединиться и использовать протоколы идентификации мошеннических схем друг друга. Если банк, оператор или государство идентифицировал мошенника, он «окрашивается» — и все остальные в моменте блокируют операции по этому номеру (Григоренко Дмитрий, Правительство РФ).

Из 300 банков в стране лишь 6 покупают антифродовое решение операторов за 2 миллиона рублей в месяц (МТС). Чтобы ускорить объединение участников рынка, необходимы государственные стимулы — льготы банковскому сектору и телекому за использование защитных решений (Касперский Евгений, Лаборатория Касперского; Галактионова Инесса, МТС).

> *«Создана антифрод-платформа — система, которая вынудила всех участников рынка объединиться и использовать протоколы идентификации мошеннических схем друг друга. Если банк, оператор или государство идентифицировал мошенника, он окрашивается как мошенник — и все остальные в моменте блокируют операции по этому номеру.»*
>
> *(Григоренко Дмитрий, Правительство Российской Федерации)*

8.5 Уголовная ответственность за «дроппинг» и сим-боксы

С сентября введена уголовная ответственность за передачу сим-карт третьим лицам для использования в преступной деятельности, а также за организацию сим-боксов и виртуальных АТС. Это дополнительный инструмент разрушения инфраструктуры кибермошенничества.

Трансграничность мошенничества делает оперативное раскрытие по горячим следам практически невозможным: организатор находится за рубежом, переводы идут через системы быстрых платежей, и к моменту обращения в полицию деньги уже за пределами России (Храпов Андрей, МВД).

9. Международное измерение и кооперация

9.1 Россия как экспортёр модели кибербезопасности

Российская система защиты от кибермошенничества признана одной из лучших в мире — многие страны берут её на вооружение. Объединённая система имеет, по оценке Касперского, «обалденный экспортный потенциал». Российские технологические и цифровые решения, несмотря на санкции, конкурируют на мировом уровне и продаются за рубежом.

Positive Technologies реализует страновые проекты — страновой межсетевой экран, страновой антифрод, страновая цифровая платформа — уже в нескольких дружественных государствах. Экспортная выручка компании по кибербезопасности: 2% два года назад, 3% год назад, прогноз на 2026 год — 5%. Рынок российского кибербеза оценивается в 360 миллиардов рублей со средним темпом роста около 20% (Филиппов Максим, Positive Technologies).

> *«Российская система защиты от этого вида преступности признана многими, даже с противной стороны, одной из лучших в мире. Многие страны уже последние полгода берут на вооружение те решения, которые мы приняли, и внедряют их у себя.»*
>
> *(Храпов Андрей, МВД России)*

9.2 Стратегия «суверенной цифры» для дружественных стран

Positive Technologies предложила дружественным странам не продажу продуктов, а передачу компетенций для создания собственных суверенных компаний и индустрий кибербезопасности. Через 4 года у страны появляется своя компания, через 5 лет — своя индустрия. Когда у 40–50 стран появятся суверенные системы кибербезопасности, выстроенные по единым лекалам, возникает качественно новый уровень глобальной устойчивости.

Кибериспытания предлагаются как инструмент международной кооперации: хакеры дружественных стран пробуют взламывать системы партнёров и наоборот, создавая соревнование и взаимное доверие (Максимов Юрий, Positive Technologies).

> *«Мы приходим к нашим друзьям и говорим: давайте делать это вместе. Ваши хакеры пробуют взламывать наши организации, наши — ваши. Сразу возникает соревнование. Ты приходишь не с буклетом, а с демонстрацией.»*
>
> *(Максимов Юрий, Positive Technologies)*

9.3 Кооперация в пространстве СНГ

Кибермошенничество носит трансграничный характер: Россия, Беларусь и Казахстан сильно вовлечены в общую проблематику. В Беларуси создана автоматизированная система обработки инцидентов с реагированием за десятки минут; Таджикистан и Узбекистан подписали соглашения о координации антимошеннических действий.

Таджикистан предложил создать в рамках РСС платформу мониторинга для всех стран региона — с постоянным доступом и отслеживанием актуальных киберугроз в реальном времени. Если один из участников процесса не успевает внедрять практики, это подвергает риску всю систему: безопасность определяется самым слабым звеном (Залесский Кирилл, Нацбанк Беларуси).

> *«Кибермошенничество носит трансграничный характер: Россия, Беларусь и Казахстан очень сильно вовлечены в эту проблематику. Борьба с кибермошенничеством требует объединения усилий: обмена лучшими практиками, взаимодействия операторов и регуляторов, оперативного обмена информацией и блокирования вредоносного трафика.»*
>
> *(Залесский Кирилл, Национальный банк Республики Беларусь)*

9.4 Россия — Индия и Россия — ОАЭ: новые треки

В сфере технологий — умных городов, кибербезопасности и ИИ — возможности для сотрудничества России и Индии огромны (Кумар Винай). Индийские партнёры создают ситуационный центр кибербезопасности в Махараштре — специализированный симуляционный сектор для подготовки специалистов в искусственной среде.

Технологии кибербезопасности, шифрования и доверенной связи, отточенные в условиях санкций, пользуются большим спросом у стран Глобального Юга, в том числе в ОАЭ: эти страны понимают, что Россия прошла «боевую проверку» (Попова Наталья). Несмотря на более 30 000 санкций, Россия демонстрирует способность создавать устойчивую цифровую инфраструктуру и киберзащиту.

9.5 Геополитическое измерение: киберконфликты и международное право

Мы вошли в эпоху глобальных киберконфликтов — и выйдем из неё нескоро. Кибератака на критическую инфраструктуру может нанести сопоставимый или больший ущерб, чем тактическое ядерное оружие — при этом она анонимна, дешевле и не пересекает юридических красных линий ядерного сдерживания (Горелкин Антон, Госдума).

Создание единого органа по кибербезопасности на международном уровне остаётся нереализованной идеей из-за межведомственных и межгосударственных противоречий. Международная кооперация

нескольких десятков стран должна быть построена так, чтобы локальные конфликты не обрушивали общую архитектуру (Кузнецов Станислав, Сбербанк; Максимов Юрий, Positive Technologies).

10. Игроки темы: компании и спикеры ПМЭФ-2026

10.1 Государственные регуляторы

Дмитрий Григоренко (Заместитель Председателя Правительства РФ) — возглавил координационный штаб по реагированию на киберинциденты; модерировал сессию «Кибермошенничество: кому платить по счетам?» (161858), зафиксировал первый перелом тренда по снижению мошенничества и представил антифрод-платформу как системное достижение.

Виталий Лютиков (Первый заместитель директора ФСТЭК России) — представил статистику уязвимостей поднадзорных организаций (54% с критическими уязвимостями на периметре), кейс Якутии под DDoS-атакой и проблему унаследованного иностранного оборудования без поддержки.

Андрей Храпов (Заместитель Министра внутренних дел) — представил статистику снижения киберпреступности на 11,8%, кейс ликвидации «Гласа Бога», информацию об уголовной ответственности за передачу сим-карт; констатировал признание российской антифрод-системы мировыми лидерами.

Антон Горелкин (Первый заместитель председателя профильного комитета Госдумы, РОЦИТ) — описал наступательную кибердоктрину США, коммерциализацию DDoS как сервиса, предложил связать государственные льготы с уровнем кибербезопасности компании.

Артём Шейкин (Первый заместитель председателя комитета Совета Федерации) — обозначил угрозу дипфейков для политической системы, необходимость развития критического мышления как ключевой меры защиты.

Виктор Евтухов (Начальник Управления Президента РФ по государственной политике в сфере ОПК) — предупредил о рисках полной автоматизации КИИ и необходимости ИИ-ответа на ИИ-атаки.

Айсен Николаев (Глава Республики Саха, Якутия) — представил кейс масштабной DDoS-атаки и ответные меры по созданию центра кибербезопасности; обозначил уязвимость электроэнергетики через её полную зависимость от цифрового управления.

Алексей Ересько (Заместитель Министра строительства и ЖКХ) — описал специфику кибербезопасности ЖКХ с 11 000 разрозненных организаций, анонсировал создание двух центров кибербезопасности отрасли.

10.2 Промышленность и КИИ

Фёдор Опадчий (Председатель правления СО ЕЭС) — представил данные о 7-кратном росте атак на ОПК, модель зонтичной защиты и семь принципов кибербезопасности для объектов электроэнергетики.

Николай Лишин (Заместитель руководителя ФМБА, член НЭС Совета Безопасности) — обозначил медицину как особо чувствительную отрасль для кибератак, проблему импортных ИИ-систем в медицине как потенциального инструмента атаки, анонсировал создание отраслевого центра

безопасности ФМБА совместно с Positive Technologies.

Юрий Жданов (Исполнительный секретарь Координационного совета генеральных прокуроров СНГ) — предупредил о дефиците специалистов по цифровым преступлениям, подтвердил личным опытом убедительность дипфейков, призвал к международной координации.

10.3 Банки и финтех

Станислав Кузнецов (Заместитель Председателя Правления ПАО Сбербанк) — наиболее активный спикер ПМЭФ-2026 по теме кибербезопасности: представил концепцию цифрового иммунитета, статистику по дипфейкам (рост в 26 раз), проект «Алитея», инициировал создание координационного штаба. Впервые в российской публичной практике призвал к открытости об инцидентах.

Сергей Цикалюк (Председатель совета директоров Страхового Дома ВСК) — публично раскрыл детали атаки на ВСК 12 ноября: сумму выкупа (около 1 млрд руб.), потери (около 900 млн руб. по марже), вектор входа (аудитор-партнёр), переговоры с вымогателями; анонсировал разработку страхового продукта от киберрисков.

Инесса Галактионова (Генеральный директор ПАО «МТС») — представила антифрод-решение МТС Защитник с распознаванием видеодипфейков за 3 секунды, статистику снижения мошеннических звонков на 40%; обозначила проблему низкого проникновения антифрод-инструментов среди банков.

Влад Федулов (Управляющий директор Авито) — обозначил опасность перекоса ответственности на операторов и банки как стимул для новой волны страхового мошенничества, описал историю глобального распространения дипфейков через мессенджеры из Латинской Америки.

10.4 Кибербез-вендоры

Евгений Касперский (Генеральный директор АО «Лаборатория Касперского») — описал три класса угроз (кражи, саботаж, шпионаж), перспективы конструктивной безопасности и неломаемых систем, поддержал идею государственных льгот за использование защитных решений, оценил экспортный потенциал российской антифрод-системы.

Борис Симис (Заместитель генерального директора Positive Technologies) — сформулировал ключевые тезисы смены парадигмы: кибербезопасность как культурный процесс, ИБ без первого лица невозможна, компании держатся только пока до них «не дошли руки», ИИ повысит возможности атакующих на два порядка.

Дмитрий Самарцев (Директор BI.ZONE) — представил ключевую статистику угроз: каждая пятая компания взломана и не знает, злоумышленники в инфраструктуре более полугода, средний ущерб от атаки не менее 50 млн руб., рост ИИ-атак на 90%+.

Юрий Максимов (Positive Technologies) — представил стратегию передачи компетенций дружественным странам, концепцию «суверенной цифры», кибериспытания как инструмент международной кооперации, прорыв по кибербезопасности энергетики.

11. Сводная таблица ключевых метрик

Показатель	Значение	Источник
Доля российских компаний, взломанных без собственного ведома	20% (каждая пятая)	(Самарцев Дмитрий, BI.ZONE)
Типичное время незамеченного присутствия злоумышленника в инфраструктуре	Более 6 месяцев, нередко годами	(Самарцев Дмитрий, BI.ZONE)
Доля атак с целями шпионажа/кражи информации	Более 40%	(Самарцев Дмитрий, BI.ZONE)
Средний ущерб от успешной корпоративной кибератаки	Не менее 50 млн руб.	(Самарцев Дмитрий, BI.ZONE)
Рост кибератак с применением ИИ за 2025 год	+90%+	(Самарцев Дмитрий, BI.ZONE)
Потери ВСК от кибератаки 12 ноября (по марже)	Около 900 млн руб.	(Цикалюк Сергей, ВСК)
Требование выкупа злоумышленников к ВСК	Около 1 млрд руб.	(Цикалюк Сергей, ВСК)
Доля поднадзорных ФСТЭК организаций с критическими уязвимостями на периметре	54%	(Лютиков Виталий, ФСТЭК России)
Доля без двухфакторной аутентификации для привилегированных пользователей	69%	(Лютиков Виталий, ФСТЭК России)
Уязвимости Fortigate за последний год	120 (около 10% активно эксплуатируются)	(Лютиков Виталий, ФСТЭК России)
DDoS-атака на Якутию (май)	10 суток, 1400+ эпизодов	(Лютиков Виталий, ФСТЭК России)
Рост атак на предприятия ОПК	В 7 раз	(Опадчий Фёдор, СО ЕЭС)
Рост числа дипфейков за полтора года	В 26 раз	(Кузнецов Станислав, Сбербанк)
Ущерб от дипфейков (текущий год, на момент сессии)	Более 2 млрд руб.	(Кузнецов Станислав, Сбербанк)
Стоимость создания одного дипфейка	Не более 50 руб.	(Кузнецов Станислав, Сбербанк)
Средний чек хищения при применении дипфейка	16 млн руб. с одной атаки	(Кузнецов Станислав, Сбербанк)
Дипфейк-заготовок в теневом интернете	Более 40 000	(Кузнецов Станислав, Сбербанк)
Прогноз потерь от дипфейков в России к концу 2026 года	250 млрд руб.	(Анастасия, проект «Алитея», Сбербанк)
Ущерб от кибермошенничества в 2025 году (МВД)	195 млрд руб.	(Скабеева Ольга / Храпов Андрей, МВД)
Доля возвращённых жертвам средств от ущерба	Около 1% (1,7 млрд руб.)	(Скабеева Ольга, Россия 1)
Снижение числа мошеннических атак (янв–дек 2025)	С 9000 до 6000 в неделю (–33%)	(Храпов Андрей, МВД)

Показатель	Значение	Источник
Снижение общего объёма киберпреступлений	−11,8%	(Храпов Андрей, МВД)
Снижение мошеннических звонков (МТС)	−40%	(Галактионова Инесса, МТС)
Ущерб от одного пробивочного сервиса «Глас Бога»	13 млрд руб. (15 000 жертв)	(Храпов Андрей, МВД)
Маржинальность дистанционных мошенничеств vs традиционных	В 4 раза выше	(Негляд Герман / данные Интерпола)
Оценка российского рынка кибербезопасности	360 млрд руб.	(Филиппов Максим, Positive Technologies)
Средний темп роста рынка кибербезопасности	Около 20% в год	(Филиппов Максим, Positive Technologies)

12. Источники

- **Стресс-тест в реальном времени: как не потерять миллиарды при кибератаке**
  День 2 · forum_id=157236
  https://forumspb.com/programme/business-programme/157236/
- **Цифровая устойчивость экономики в эпоху глобальных киберконфликтов**
  День 1 · forum_id=156679
  https://forumspb.com/programme/business-programme/156679/
- **Цифровой самозванец: новое оружие массового поражения**
  День 2 · forum_id=157239
  https://forumspb.com/programme/business-programme/157239/
- **Кибермошенничество: кому платить по счетам?**
  День 3 · forum_id=161858
  https://forumspb.com/programme/business-programme/161858/
- **Цифровое будущее: общие векторы развития, вызовы и решения**
  День 1 · forum_id=156764
  https://forumspb.com/programme/business-programme/156764/
- **Международная кооперация: технологии без людей, как люди без технологий**
  День 1 · forum_id=156761
  https://forumspb.com/programme/business-programme/156761/
- **Цифровой суверенитет под ключ: взаимовыгодные перспективы**
  День 1 · forum_id=156670
  https://forumspb.com/programme/business-programme/156670/
- **Инвестиции в новые рынки: как меняется ландшафт в эпоху неопределенности**
  День 1 · forum_id=156592
  https://forumspb.com/programme/business-programme/156592/
- **Созидатели: экономика сквозь призму технологического суверенитета страны**
  День 1 · forum_id=156637
  https://forumspb.com/programme/business-programme/156637/
- **Россия – Индия**
  День 2 · forum_id=156686
  https://forumspb.com/programme/business-programme/156686/
- **Россия и ОАЭ: новые пути технологического взаимодействия**
  День 2 · forum_id=156899
  https://forumspb.com/programme/business-programme/156899/

- **Цифровые дети, кто за вас в ответе?**
  День 2 · forum_id=156639
  https://forumspb.com/programme/business-programme/156639/
- **Твои слова как пули: как информация превратилась в мощнейшее оружие современности**
  День 2 · forum_id=156645
  https://forumspb.com/programme/business-programme/156645/
- **Технологический прорыв и трансформация контрольно-надзорной деятельности: новое качество регулирования**
  День 3 · forum_id=157235
  https://forumspb.com/programme/business-programme/157235/
- **Будущее для каждого, благо для всех: как управлять конкуренцией за ресурсы и пространства**
  День 1 · forum_id=156593
  https://forumspb.com/programme/business-programme/156593/

По материалам деловой программы ПМЭФ-2026. Все цифры и формулировки приведены строго по выступлениям спикеров. Подготовлено АНО «Цифровые платформы».