ЦИФРОВИЗАЦИЯ СО ШКОЛЬНОЙ СКАМЬИ

В ЛИЦЕЕ №369 В КРАСНОСЕЛЬСКОМ РАЙОНЕ САНКТ-ПЕТЕРБУРГА ИДЕТ ЭКСПЕРИМЕНТ, КОТОРЫЙ МОЖЕТ ПОВЛИЯТЬ НА ЦИФРОВИЗАЦИЮ РОССИЙСКИХ ШКОЛ. ЗДЕСЬ ТЕСТИРУЮТ ПЛАНШЕТЫ KVADRA_T ОТ ПРОИЗВОДИТЕЛЯ КОМПАНИИ YADRO — УСТРОЙСТВА СОЗДАНЫ СПЕЦИАЛЬНО ПОД ЗАДАЧИ ОБРАЗОВАНИЯ. СЕЙЧАС В ЛИЦЕЕ ЕЖЕДНЕВНО РАБОТАЕТ ОКОЛО ПЯТИ СОТЕН РАЗНЫХ ПЛАНШЕТОВ, ВСЕГО ИХ ПОЧТИ ШЕСТЬСОТ. ЭТО ПОЗВОЛИЛО НЕ ПРОСТО ПРОВЕРИТЬ, НАСКОЛЬКО ТЕХНИКА УДОБНА ДЛЯ УЧЕБЫ, НО И ПОНЯТЬ, КАКИМ ДОЛЖЕН БЫТЬ «ШКОЛЬНЫЙ» ПЛАНШЕТ, ЧТОБЫ СТАТЬ РЕАЛЬНО ПОЛЕЗНЫМ ИНСТРУМЕНТОМ. КСЕНИЯ АХМЕТЖАНОВА

Планшет KVADRA_T, произведенный на крупнейшем в России заводе полного цикла «Ядро Фаб Дубна», работает под управлением собственной мобильной операционной системы kvadraOS. В систему интегрирован магазин приложений RuStore, поэтому она совместима с широким спектром программ и устройств. Как рассказали в компании, перед тем как внедрить планшет в образовательный процесс, они выслушали пожелания учителей. Педагоги обратили внимание на скорость работы устройства, его энергоемкость (устройство должно выдерживать шесть уроков подряд), при этом гаджет должен иметь большой экран и удобный интерфейс, где все нужные приложения «уже под рукой».

«Наличие собственной операционной системы kvadraOS позволяет команде проекта гибко реализовывать такие требования и подстраивать решения под учебные нужды. Сегодня многие педагоги пользуются личными телефонами для работы: проверяют домашние задания, кидают материалы в чаты, управляют презентациями. Новый планшет должен заменить все эти решения одним простым и надежным устройством»,— добавляют в пресс-службе компании YADRO.

Когда начинается занятие по какому-либо предмету, планшет автоматически запускает нужный



ПРЕСС-СЛУЖБА YADRO

ПЛАНШЕТНЫЕ РЕШЕНИЯ, ЦИФРОВЫЕ ПАНЕЛИ, СИСТЕМЫ ОНЛАЙН-ПРИСУТСТВИЯ, ЭКОСИСТЕМЫ — ЭТО ВСЕ ТО, ЧТО ПОЗВОЛЯЕТ РЕБЕНКУ РАЦИОНАЛЬНО И ЭФФЕКТИВНО ИСПОЛЬЗОВАТЬ ВРЕМЯ СВОЕГО ДЕТСТВА, КОТОРОЕ ПРОХОДИТ В ШКОЛЕ

набор приложений — учителю не нужно тратить время на подготовку. Еще одним интересным результатом эксперимента стала идея планшета как «пульта управления классом». Учитель больше не привязан к рабочему столу — он может ходить по классу, фотографировать лабораторные опыты, показывать материалы прямо с планшета на большую доску или на устройства учеников, что формирует интерактивную атмосферу в классе.

В процессе тестирования появились и более «земные» находки: учителям понадобились стилусы с очень тонким наконечником, чтобы писать формулы, и надежное крепление для них — магнитные держатели не выдержали школьного ритма. Также учителя запросили предоставить им полноценную клавиатуру, чтобы можно было быстро работать с отчетами и журналами.

Как рассказал директор лицея №369 и член Общественной палаты города Константин Тхостов, сейчас на базе образовательного учреждения тестируют комплексные решения от отечественного производителя, которые не ограничиваются только планшетами.

«Реальная цифровая экономика предопределена цифровыми возможностями современных образовательных систем. Поэтому планшетные решения, цифровые панели, системы онлайн-присутствия, экосистемы — это все то, что позволяет ребенку рационально и эффективно использовать время своего детства, которое проходит в школе. Плюс ко всему эти системы позволяют учителю развиваться и избегать профессионального выгорания»,— комментирует господин Тхостов.

Как отмечают представители YADRO, главная идея проекта — не подгонять учебный процесс под готовое устройство, а создать устройство под реальные школьные задачи. Такой подход оказался выигрышным: он дает учителям то, что действительно нужно, а не просто новое «железо». При этом в компании не исключают, что проект в перспективе может вырасти в масштабное решение с экспортным потенциалом.

«Рост оснащенности учебных заведений современными планшетами и ноутбуками постепенно меняет формат уроков, превращая их в более интерактивные и гибкие. Однако полное внедрение и широкое использование цифровых платформ все еще остаются задачей будущего. При этом отечественные производители могут сыграть ключевую роль, предложив решения, адаптированные под потребности системы образования»,— рассуждает ведущий аналитик Mobile Research Group Эльдар Муртазин. ■

4 → **ЦЕНА УЯЗВИМОСТИ** В 2025 многие компании увеличили свои бюджеты на обеспечение ИБ. «Это связано с ростом количества угроз, необходимостью импортозамещения ИБ-решений, а также с ужесточением законодательства в части КИИ и ПДн. Кроме того, начал расти спрос на ИБ-аудит. Полагаю, что тренд продолжится и в 2026 году, однако рост будет умеренным»,— говорит госпожа Белоусова.

Евгений Акимов, директор направления развития бизнеса департамента информационной безопасности группы Rubytech, солидарен с тем, что во многом расходы на обеспечение кибербезопасности в последние три года были связаны с необходимостью импортозамещения.

«Это привело к отставанию во внедрении новых механизмов и технологий киберзащиты. Поэтому, несмотря на то, что большинство проектов по импортозамещению близко к завершению, высвобождающиеся ресурсы позволят усилить оснащенность команд кибербезопасности. А самые громкие и критичные публичные инциденты дадут возможность обосновать некоторый рост бюджетов, однако вряд ли он превысит 10–15%»,— думает господин Акимов.

По оценкам госпожи Ледяевой, в 2025 году бюджеты на ИБ в целом росли, но рост был сдержанным. «По данным аналитиков, глобальные траты увеличились, однако для большинства компаний это выглядело как прибавка на уровне 4–8%. Часто деньги шли не на развитие, а на поддержание текущего уровня защиты. При этом ИБ-команды сталкивались с ситуацией, когда угрозы росли быстрее, чем доступные бюджеты и ресурсы»,— указывает она.

В 2026 году эксперт ожидает продолжения роста расходов на ИБ, в среднем на 5–10%, но без резких скачков. «Компании будут более осознанно вкладываться в устойчивость: предотвращение инцидентов, готовность к атакам и работу с человеческим фактором через обучение и тренировки. На фоне общего роста трат ИБ будет рассматриваться не как отдельная статья, а как обязательная часть цифрового развития бизнеса»,— подчеркивает госпожа Ледяева.

Господин Богданов также замечает, что в 2025 году рост бюджетов на информационную безопасность замедлился. «Высокая ключевая ставка и общая экономическая неопределенность заставили бизнес пересмотреть инвестиционные планы, сместив акцент с масштабных проектов внедрения на оптимизацию текущих расходов»,— объясняет он.

В 2026 году значительного увеличения финансирования он также не ожидает. «Бюджеты, с высокой долей вероятности, останутся на уровне 2025 года или покажут чисто номинальный рост, несмотря на объективное усложнение угроз. Это означает, что главным трендом станет не привлечение новых средств, а повышение эффективности каждого вложенного рубля. В выигрыше останутся компании, которые сделают ставку на тонкую настройку, консолидацию решений и сервис-ориентированные модели»,— полагает Валентин Богданов.

По данным Константина Горбунова, большинство российских компаний не планируют сокращать расходы на информационную безопасность в 2026 году. «32% компаний оставят расходы на прежнем уровне, 32% — увеличат. Сокращение планируют лишь 7% организаций. Основные направления инвестиций в 2025–2026 годах — защита персональных данных, замена продуктов ушедших вендоров и защита КИИ. При этом у многих компаний есть стратегия развития ИБ, что указывает на более осмысленный подход к распределению бюджета»,— говорит господин Горбунов.

УСКОРЕНИЕ ВСЕГО Кирилл Митрофанов считает, что существенных изменений в ландшафте угроз в 2026 не ожидается. «Мы предполагаем, что злоумышленники будут эволюционировать, развивать технические навыки и инструментарий. Продолжится рост числа атак на разработчиков ПО и небольших подрядчиков, которые часто используются как точка входа в более крупные компании»,— полагает он.

По мнению Валентина Богданова, в 2026 году главным приоритетом станет получение максимальной отдачи от уже сделанных инвестиций в IT и ИБ через повышение операционной эффективности. «Фокус сместится с закупки новых решений к максимизации отдачи от ранее внедренных инструментов. Компании будут проводить тотальный аудит и „харденинг“ своей защиты: анализировать, все ли возможности ИБ-решений задействованы, и проверять системы на наличие старых, оставшихся без техподдержки сервисов и прочих рисков. Цель — закрыть основные уязвимости за счет грамотной настройки, а не дополнительных капитальных затрат. Экономическое давление и поиск операционной эффективности закономерно подтолкнут рынок к сервис-ориентированной модели безопасности, где аутсорсинг функций ИБ станет способом получить экспертизу и предсказуемые расходы»,— рассуждает он.

По прогнозам Алины Ледяевой, в 2026 году фокус атак сместится с «железа» на учетные записи, включая сервисные аккаунты и API-ключи в облаке. «ИИ продолжит делать социнженерию дешевле и убедительнее: письма, звонки и голосовые дипфейк-сценарии будут выглядеть еще более правдоподобно и чаще вводить сотрудников в заблуждение. Шифровальщики сохранятся как один из ключевых рисков, поскольку они могут останавливать процессы и создавать давление на бизнес. Дополнительные риски будут создавать подрядчики, интеграции и внешние сервисы, через которые атаки проще масштабировать»,— говорит она.

Евгений Акимов также называет главным трендом массовое использование искусственного интеллекта злоумышленниками для проведения кибератак. «Первые успешные случаи применения ИИ в атаках были зафиксированы уже в 2025 году, а в 2026-м следует ожидать их резкого роста. Это связано с тем, что ИИ радикально снижает порог входа в киберпреступность. Сложные многоступенчатые атаки, которые раньше могли организовать только высококвалифицированные хакеры, теперь становятся доступны практически любому. Искусственный интеллект автоматизирует разведку, подбор уязвимостей, создание вредоносного кода и даже социальную инженерию. Это означает, что организации столкнутся с лавиной профессионально выполненных атак при минимальных затратах со стороны злоумышленников»,— прогнозирует он.

Главный тренд 2026 года — ускорение всего: атак, реакции, последствий, резюмирует Евгений Семенов. «ИИ продолжит усиливать злоумышленников, снижая порог входа и увеличивая скорость подготовки атак. Поверхность атаки будет расширяться за счет API, интеграций и экосистемных моделей»,— прогнозирует он. Отдельно господин Семенов выделяет кадровый и управленческий риски. «Без встроенной ИБ-логики в процессы и продукт устойчивость становится недостижимой: ручное реагирование и героизм больше не работают»,— заключает эксперт. ■