

ОБЩЕСТВО  
22 МАЯ 2026, 14:35

## В Минске прошла вторая конференция "День практической кибербезопасности от МТЕ"



Вторая конференция "День практической кибербезопасности от МТЕ" 19–20 мая собрала не только сотни профессионалов в сфере обеспечения информационной безопасности, но и тех, кто может ими стать.



Первый день форума стал настоящим открытием примерно для 250 школьников из столицы и Минского района, для которых специалисты ООО "МультиТек Инжиниринг" совместно с Министерством образования, Управлением "К" МВД Беларуси, БГУИР и ОАО "АСБ Беларусбанк" провели профориентацию. Ребята не только обсуждали вопросы цифровой гигиены,

разбирали методы защиты аккаунтов, учились отличать настоящие сайты от созданных мошенниками, но и ознакомились с перспективами профессии специалиста по кибербезопасности и тем, как начать карьеру в этой сфере.



"Культура кибербезопасности должна формироваться с детских лет. Мы вносим свой вклад в реализацию этой идеи, инвестируя в образование детей, обучая их защите данных. Уже три года совместно с партнером мы выпускаем журнал для младших школьников, посвященный теме информационной безопасности. С более старшими школьниками проводим занятия по безопасному поведению в интернете, а для старшеклассников подготовили буклет, где рассказываем об азах профессии специалистов по кибербезопасности. Мы заинтересованы, чтобы профессионалов в сфере киберзащиты становилось больше, а уровень их подготовки – выше. Ведь мы в "[МультиТек Инжиниринг](#)" и сами постоянно расширяем компетенции, чтобы быть готовыми к решению любых задач по защите данных", – отметил заместитель генерального директора Дмитрий Красницкий.



Поскольку организатором конференции выступило ООО "МультиТек Инжиниринг", более 7 лет профессионально занимающееся защитой информации, акцент был сделан на практические вопросы кибербезопасности. Во второй день форума, куда были приглашены руководители и специалисты по защите данных, представители "МультиТек

Инжиниринг" щедро делились практическим опытом проектирования, создания и сопровождения систем защиты информации.



"Эффективность систем защиты информации в значительной степени зависит от компетенций их создателей. Эти знания и навыки – результат напряженной работы, анализа допущенных ошибок и достигнутых успехов. И мы твердо уверены, что такими знаниями надо делиться со

специалистами страны, ежедневно решающими задачи по защите информации. Ведь информатизация, предоставляя организациям огромные возможности, делает данные одним из наиболее ценных активов, требующих соответствующего уровня защиты", – отметил Дмитрий Красницкий.



Позиция организаторов осталась неизменной с первой конференции: мероприятие прошло без рекламы и презентаций конкретных средств защиты информации, без участия и упоминания вендоров. Основным вопросом для обсуждения в этом году стала не только кибербезопасность, но и киберустойчивость – способность организации прогнозировать, сдерживать и противостоять киберугрозам, а также быстро и с минимальными издержками восстанавливать деловую активность после таких атак.

Фактически кибербезопасность и киберустойчивость – два взаимодополняющих направления, без которых невозможно обеспечить по-настоящему высокий уровень защиты.



"Специалисты прекрасно знают, что стопроцентной защиты не существует. Именно поэтому ["МультиТек Инжиниринг"](#) рассматривает киберустойчивость как эволюционный этап обеспечения кибербезопасности", – подчеркнул Дмитрий Красницкий.

Он также обратил внимание на то, что киберустойчивость организации напрямую влияет на ее прибыль: чем быстрее пройдет восстановление после инцидента, тем меньший ущерб он принесет. Поэтому сейчас обеспечение киберустойчивости переходит в разряд жесткого требования, основанного на следовании стандартам, регламентам, обучении пользователей, кибертренировках, мониторинге состояния безопасности, оценке угроз и принятию своевременных мер по реагированию на них.

При этом спикеры конференции рекомендовали специалистам придерживаться процессного подхода, реализуя проекты в сфере информационной безопасности. Он предполагает органичную интеграцию безопасности в основные бизнес-процессы организации. Тому, как организовать эту синергию, был посвящен ряд выступлений во второй день конференции. Обладая большим практическим опытом, специалисты "МультиТек Инжиниринг" поделились методами проектирования, внедрения и автоматизации таких процессов, как управление активами, инцидентами, оценка рисков. Спикеры конференции также представили разработанную "МультиТек Инжиниринг" методику определения приоритетов устранения уязвимостей.





С трибуны конференции много говорили о культуре информационной безопасности. В частности, об обучении не только специалистов по защите информации, но и пользователей информационных систем, руководителей бизнес-подразделений. Так называемый человеческий фактор – краеугольный камень в вопросах кибербезопасности и киберустойчивости. Неспроста методология обеспечения защищенности информации от "МультиТек Инжиниринг" включает в себя не только процессы и технологии, соответствующие всем требованиям белорусского законодательства в данной области, но и повышение уровня знаний о кибербезопасности.

Как показывают результаты расследований киберинцидентов, подавляющее большинство кибератак начинается с ошибки человека – пользователя информационной системы. Понимая, что именно люди – фундамент информационной безопасности, "МультиТек Инжиниринг" внедряет процесс обучения работников организаций-заказчиков во все проекты систем защиты информации. Так формируется "человеческий firewall", помогающий снизить реализацию инцидентов в сфере информационной безопасности, вовремя их выявить и качественно отреагировать.

Но чтобы максимально эффективно действовать в этой сфере, знания теории недостаточно. На конференции отмечена важность практических навыков и слаженных действий специалистов при отражении кибератаки и устранению ее последствий. Лучший способ научиться этому – кибертренировки.

Участникам конференции был представлен практический разбор сценария реагирования на инцидент информационной безопасности.



В ходе конференции приглашенные получили большой объем практической информации по ряду направлений кибербезопасности, а организаторы форума – множество положительных отзывов.

[Размещение рекламы на БЕЛТА](#)

**ТЕГИ**  
[Беларусь](#)