



**Андрей ЧАПЧАЕВ**  
генеральный директор  
ИнфоТекС

# ИНФОТЕКСУ — 30 ЛЕТ!

## ИСТОРИЯ КОМПАНИИ, СЫГРАВШЕЙ СУЩЕСТВЕННУЮ РОЛЬ В ИНФОРМБЕЗОПАСНОСТИ РОССИИ

**Р**ассказывает один из основателей компании ИнфоТекС, её бессменный генеральный директор Андрей Чапчаев.

### КАК ВСЕ НАЧИНАЛОСЬ

— Андрей Анатольевич, поздравляем Вас с юбилеем! Желаем и Вам и компании крепкого здоровья, активного долголетия, верных друзей и надежных партнеров! Расскажите, пожалуйста, как всё начиналось?

— Начало деятельности компании связано с введения в «гражданский» оборот технологий криптографической защиты информации. До этого криптография системно использовалась только в военной сфере и в областях, связанных с гостайной. В конце 1980-х в стране был опубликован ГОСТ 28147–89 на алгоритмы криптографической защиты информации. Коммерциализация экономики в начале 1990-х начала создавать спрос на криптографическую защиту информации, прежде всего в среде крупных структур, исторически заинтересованных в защите своих данных. Именно они первые заинтересовались «гражданской» криптографией.

Конечно, на тот момент говорить о каком-то сложившемся рынке информационной безопасности было преждевременно. Единицы были готовы вкладываться в развитие криптографических средств защиты информации. Мы были одними из первых, кто увидел и поверил в перспективы развития этого направления.

### ВРЕМЯ ИНТЕРНЕТА

Толчком, который способствовал увеличению спроса на криптографию, послужило активное подключение организаций к сети Интернет в качестве универсальной коммуникационной среды. Экономически это стало более обоснованным, чем строительство собственных выделенных сетей связи. Это же, в свою очередь, привело к активизации как отдельно взятых мошенников, так и целых преступных сообществ, нацеленных на получение конфиденциальной информации и выведение из строя элементов информационных систем путем рассылки вредоносных писем с вирусами. Все мы, например, прекрасно помним истории с открытой продажей в те годы компакт-дисков с базами данных разных ведомств на Горбушке.

Таким образом к началу 2000-х гг. сформировался спрос на построение доверенной информационно-коммуникационной среды предприятий и доверенного электронного документооборота. А в продуктовой портфеле ИнфоТекСа появилось решение «Виртуальная частная сеть ViPNet», которое и по сей день является основой многих наших продуктов.

Интересно отметить, что, когда на рубеже 2000-х наши зарубежные коллеги ставили на крыло протокол организации VPN сетей IPSec, специалисты ИнфоТекС разрабатывали и совершенствовали свой защищенный протокол — IPIir (IP layer interconnection robust), который за эти годы не только подтвердил свои высокие качества надежного VPN-протокола, но и не так давно был утвержден Росстандартом в качестве рекомендаций по стандартизации Р1323565.1.034–2020 «Информационная технология. Криптографическая защита информации. Протокол безопасности сетевого уровня». И мы, как и 20 лет назад, продолжим считать наш IPIir достойной альтернативой IPSec'у, обладающей целым рядом преимуществ.

### РКИ-ПРОДУКТЫ

В 2001–2002 гг. компания помимо развития сетевых средств безопасности: VPN-продуктов и межсетевых экранов; начинает активно работать в направлении создания собственной линейки РКИ-продуктов. В это же время создается первая дочерняя компания — ИнфоТекС

*Единицы были готовы вкладываться в развитие криптографических средств защиты информации. Мы были одними из первых, кто увидел и поверил в перспективы развития этого направления*

Интернет Траст, нацеленная на оказание услуг в области защищенного документооборота и РКИ.

### ПОДГОТОВКА СПЕЦИАЛИСТОВ

Несмотря на то что в начале 2000-х у компании было еще не так много клиентов, было принято решение вкладываться в развитие учебного направления. Мы понимали: мало просто создать продукт и выпустить его на рынок, необходимо, чтобы были специалисты, способные работать с ним. Так, на рубеже 2000-х начинает формироваться еще одно направление, связанное с собственной системой дополнительного профессионального образования и повышения квалификации. Изначально его развитием занимался отдел технической поддержки, на базе которого позднее сформировалось специализированное подразделение — отдел учебных программ.

10 лет назад с учетом роста требований к системе подготовки квалифицированных кадров в сфере ИБ (как в части содержания программ, так и методологии обучения) было сформировано отдельное юридическое лицо — НОЧУ ДПО ЦПК «Учебный центр ИнфоТекС», обладающее квалифицированными преподавательскими кадрами, набором программ подготовки и учебных материалов по разным направлениям, аккредитованное в качестве образовательного учреждения в соответствии с регуляторными требованиями в сфере образования.

### ПРОГРАММНО-АППАРАТНЫЕ КОМПЛЕКСЫ

Исходно ИнфоТекС ориентировался на разработку программных средств защиты информации, рассчитывая, что заказчик будет самостоятельно осуществлять выбор аппаратных платформ для размещения данного ПО. Такой

концепции мы придерживались до 2008 года. Когда стало ясно, что сложности информационных систем на стороне заказчиков и комплекс решаемых ими задач стал таким, что у заказчика просто не остается времени на выбор и интеграцию отдельного «железа» и программного обеспечения. Мы все чаще стали получать запросы на приобретение готовых программно-аппаратных комплексов, обеспечивающих защиту информации, поэтому в 2008 г. начали производство собственных ПАКов. Надежным поставщиком аппаратных платформ для нас стала компания «Аквариус»; кстати, это технологическое партнерство продолжается до сих пор.

### «ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ»

Очередным логическим этапом нашего продуктового развития после 2010 г. стало создание нового

### 30+ ЛЕТ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основной бизнес ИнфоТекС лежит в сфере разработки и производства высокотехнологичных программных и программно-аппаратных средств защиты информации. Но ИнфоТекС сегодня — не только вендор, это еще Группа компаний, включающая, помимо компании с «родным» названием, и такие отдельные «юридические лица», как:

- ♦ Центр повышения квалификации «Учебный центр ИнфоТекС» — негосударственное образовательное частное учреждение. Через него в год проходит свыше 1000 человек, программы обучения согласовываются и получают одобрение ФСБ и ФСТЭК, при этом по некоторым курсам длительность обучения составляет сотни часов. Выпускники учебного центра получают удостоверения государственного образца о получении дополнительного образования и повышении квалификации.

- ♦ Компания «СФБ Лаборатория», занимающаяся сертификацией средств защиты информации (СЗИ).

- ♦ Компания «Перспективный мониторинг» (ПМ), специализирующаяся на мониторинге и предотвращении компьютерных атак. Как бизнес-единица «Перспективный мониторинг» предоставляет услуги СОС для ряда крупных государственных и коммерческих структур (Московская биржа, МТС Банк, Финам, Сбербанк Страхование, Кредит Урал банк, Эльдorado и др.). При этом опыт специалистов «Перспективного мониторинга» позволяет обогащать и совершенствовать продукты ИнфоТекС, предназначенные для обнаружения и предотвращения компьютерных атак.



- ♦ «Инфотекс Интернет Траст» — аккредитованный удостоверяющий центр, входящий в пятерку крупнейших. Оператор юридически значимого электронного документооборота и сдачи электронной отчетности. Специалисты компании участвуют в создании инфраструктуры электронного ведения бизнеса, необходимой для развития отечественной экономики.

- ♦ Компания «Системы практической безопасности», специализирующаяся на разработке СКЗИ высокого класса защищенности. Ее флагманским решением является сертифицированный комплекс средств криптографической защиты информации «Квазар», предназначенный для поддержки криптографической защиты высокоскоростного обмена информацией между центрами обработки данных с использованием региональных и магистральных каналов транспортных сетей OTN.

- ♦ Совсем недавно к Группе компаний присоединилась еще одна компания — «Промышленные Криптосистемы» (ПроКСИ). Она специализируется на разработке продуктов и прикладных решений на базе технологий распределенного реестра (блокчейна) и смарт-контрактов.

продукта — системы обнаружения компьютерных атак. И тут уместно вспомнить об еще одной нашей дочерней компании «Перспективный мониторинг», созданной в то же время. Практический опыт, который получают специалисты ПМ, обеспечивая мониторинг защищенности информационных систем клиентов, имеет применение и в прикладной сфере. Например, базы решающих правил, которые используются в продуктах ИнфоТеКС, создаются и регулярно обновляются сотрудниками «Перспективного мониторинга», а значит, снижается зависимость от коммерческих сигнатур зарубежных разработчиков.

Хочу отметить, что «Перспективный мониторинг» стал первым корпоративным центром мониторинга, подключившимся к ГосСОПКА, о чем свидетельствует соглашение, заключенное в октябре 2017 г. между компанией и ФСБ России о взаимодействии в области обнаружения, предупреждения и ликвидации последствий компьютерных атак.

#### ДЛЯ ЗАЩИТЫ АСУ ТП

В 2016 г. было принято решение о создании еще одного продуктового направления, объединившего средства защиты информации для промышленных информационных систем, включая распределенные системы IIoT. В настоящее время оно представлено двумя специализированными линейками для защиты АСУ ТП: наложенными сетевыми средствами, выполненными в виде шлюзов безопасности в промышленном исполнении, и встраиваемыми средствами криптографической защиты. Совместно с нашими продуктами и решениями корпоративного класса они закрывают большинство требований по защите объектов КИИ.

Существенным достижением в данном направлении стала разработка нами специализированного криптопротокола, предназначенного для защиты информационного обмена между элементами АСУ, M2M- и IIoT-устройствами. Протокол получил название CRISP. Приказом № 1504-ст Федерального агентства по техническому регулированию и метрологии от 30.12.2019 были утверждены рекомендации по стандартизации этого протокола.

Особенностью данного протокола является его небольшая избыточность, так как он ориентирован на обработку небольших объемов информации, специфичных для АСУ и универсальность — независимость от используемых в конкретной АСУ протоколов транспортного уровня. Это позволяет ему быть более эффективным, чем стандартные протоколы, пришедшие из классических ИТ. При этом в зависимости от поставленных задач протокол способен обеспечивать конфиденциальность (шифрование), целостность и аутентичность защищаемых данных как одновременно, так и каждое из этих свойств отдельно. Так, например, в сфере АСУ ТП целостность данных чаще оказывается гораздо важнее их конфиденциальности.

#### СФБ ЛАБ

Разрабатывая многие годы широкий спектр СКЗИ и занимаясь их сертификацией по требованиям ФСБ, мы накопили большой опыт, вылившийся на рубеже 2020 г. в создание новой компании в группе компаний «ИнфоТеКС» — специализированной исследовательской лаборатории СФБ Лаб. В настоящее время СФБ Лаб является аккредитованной ИЛ ФСБ России и может проводить весь комплекс тематических и специальных исследований СКЗИ любого класса защищенности.

#### НАДЕЖНЫЕ ПАРТНЕРЫ

Отдельно хочу отметить нашу тесную партнерскую работу с компанией «Системы Практической Безопасности» (СПБ) — коллеги являются высококлассными специалистами в области создания сетевых шифраторов высоких классов защищенности. Но первой нашей совместной работой стала работа в другом направлении: создание специализированного решения для банков — отечественного платежного HSM — криптографического ядра любой современной платежной системы. Поэтому вхождение компании СПБ в 2018 г. в состав ГК «ИнфоТеКС» стало для нас всех вполне логичным шагом, доказывающим нашу совместную устремленность на создание уникальных и

востребованных рынком продуктом, особенно в свете активно идущих процессов импортозамещения.

В 2020 году ГК «ИнфоТеКС» пополнилась еще одной инновационной компанией «Промышленные криптосистемы» — специалистами по платформам распределенных реестров. Нет, это совсем не про криптовалюты. Это про системы корпоративного класса, позволяющие организациям эффективно оптимизировать свою деятельность, переводя свои бизнес-процессы, включающие взаимодействие со множеством контрагентов, в форму смарт-контрактов. Конечно, мы бы не были ИнфоТеКС, если бы не реализовали для всего этого правильной криптографии.

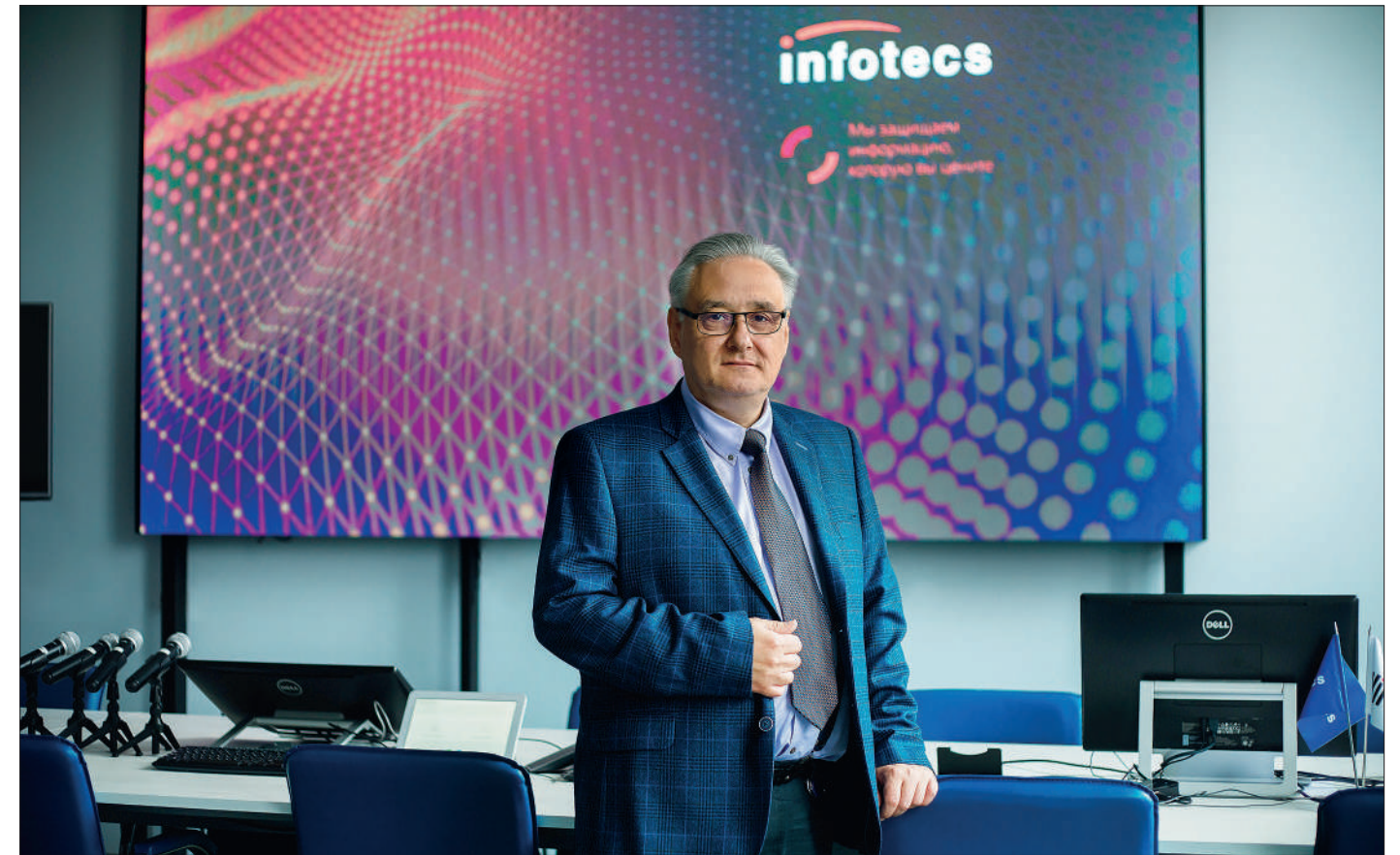
#### УСТРЕМЛЕННОСТЬ В БУДУЩЕЕ. НА НОВОМ ВИТКЕ

Подводя итог нашего небольшого исторического экскурса, хочу отметить, что ИнфоТеКС нацелен не только на решение текущих задач по защите информации. Мы смотрим в будущее и вкладываем немалые усилия и средства в научные разработки. Знаковым событием для нас стало заключение в 2017 году соглашения с физическим факультетом МГУ им. М.В. Ломоносова. Это партнерство привело к появлению опытных образцов аппаратуры квантовой криптографии, основанной на технологии квантового распределения ключей. Сейчас ИнфоТеКС находится на этапе сертификации первых квантовых разработок. В наших ближайших планах — вывести свои продукты на массовый рынок.

Можно сказать, что на очередном витке развития ИнфоТеКС вернулся к своим истокам — к криптографии, но уже на новом уровне, когда гарантии защиты информации обеспечиваются фундаментальными физическими принципами, а не ресурсоемкой математикой.

При этом опыт производства рыночных продуктов, накопленный ИнфоТеКС более чем за два десятилетия, позволил компании за короткий срок воплотить научные идеи в реальное «железо».

В этом направлении компания ставит перед собой глобальные и довольно амбициозные цели — создание



коммерческих продуктов, которые могли бы стать основой для будущих перспективных квантовых сетей связи России.

#### НОРМОТВОРЧЕСТВО И СТАНДАРТИЗАЦИЯ

— Выше мы упоминали о протоколах IPIR и CRISP — результате многолетней работы специалистов компании. Какую еще работу на поле нормотворчества и стандартизации ведет ИнфоТеКС?

— За 30 лет выстроено плодотворное взаимодействие с регуляторами, профильными комитетами Росстандарта и профессиональным сообществом в целом по вопросам стандартизации и нормотворчества в сфере ИБ.

Так, в техническом комитете по стандартизации ТК № 26 «Криптографическая защита информации» ИнфоТеКС выполняет роль секретарской компании, обеспечивая деятельность комитета и регулярно собирая экспертов на своей площадке для обсуждения актуальных вопросов развития криптографии и ее стандартизации.

Специалисты компании являются активными участниками ТК 362 «Защита информации», а также подкомитета № 1 «Безопасность финансовых (банковский) операций» Технического комитета по стандартизации № 122 «Стандарты финансовых операций» ЦБ России.

Кроме этого, эксперты ИнфоТеКС участвуют в работах Консультативного совета Роскомнадзора, входят в состав экспертного совета Минцифры по отечественному ПО, а также являются членами ряда общественных организаций: Ассоциации документальной электросвязи (АДЭ), АРПП «Отечественный софт», АПКИТ и пр. Учебный центр ИнфоТеКС помогает в разработке федеральных государственных образовательных стандартов и профессиональных образовательных стандартов в области информационной безопасности.

Отдельно хочется подчеркнуть наше активное участие в международной организации по стандартизации ИСО (ISO), в том числе в комитете ISO/TC 307 Blockchain and distributed ledger

technologies, который занимается стандартизацией в области блокчейн-технологий. Наши специалисты содействуют разработке международных стандартов и принятию российских национальных стандартов криптографической защиты в качестве международных.

#### ИСТОРИЯ С ГЕОГРАФИЕЙ

— Расскажите о географических аспектах жизни компании. Как ИнфоТеКС осваивает Россию?

— 30 лет назад ИнфоТеКС начинался как объединение нескольких единомышленников, верящих в то, что «гражданская» криптография будет востребована. Сегодня в компании трудится более 1500 человек, а ее представительства открыты от Санкт-Петербурга до Хабаровска.

Наша географическая экспансия тесно связана с расположением крупного бизнеса в России, научных школ в области прикладной математики (информатики) и центров регионального управления. В настоящее время группа компаний — это сеть территориально распределенных офисов, наши

представительства есть во многих крупных городах: в Томске, Хабаровске, Новосибирске, Екатеринбурге, Уфе, Ростове-на-Дону, Пензе.

В Москве находится центральное подразделение компании, второй по масштабам офис располагается в Санкт-Петербурге.

Такая территориальная распределенность позволяет нам быть более устойчивыми. Приведу свежий пример: недавно у московского офиса случился внеплановый переезд, тем не менее это никак не сказалось на планах разработки продуктов или на научной деятельности. Разработка, тестирование, коммерческий блок — все это давно уже не консолидировано только в столицах.

Хочу отдельно подчеркнуть тот вклад, который вносят в развитие ИнфоТеКС наши партнеры — системные интеграторы, поставляющие и поддерживающие решения компании по всей России и в странах СНГ.

На данный момент в партнерскую сеть входит более 200 компаний, а также несколько десятков компаний — технологических партнеров, с которыми ИнфоТеКС совместно разрабатывает и поставяет на рынок комплексные решения в области информационной безопасности.

### «КАДРОВАЯ ПРОБЛЕМА НАМ НЕ ЗНАКОМА»

— Как мы знаем, на рынке ИБ и ИТ сейчас наблюдается жесткий кадровый голод. Как компания «ИнфоТеКС» решает для себя эту проблему?

— Предвидя данную проблему, мы довольно давно запустили проект «ИнфоТеКС Академия», который сейчас

является для компании своего рода кузницей кадров. Он включает две программы: грантовую и стажировочную.

Грантовая программа рассчитана на поддержку студенческих научных коллективов. Мы выделяем деньги молодым специалистам на развитие их идей и реализацию проектов, которые потом проходят апробацию на пригодность их интеграции в продукты и решения ИнфоТеКС.

Стажировочная площадка дает возможность студентам получить опыт реальной разработки без отрыва от учебы. Стажеры получают стипендию от компании, а самые успешные приглашены стать ее частью после прохождения программы. Хочу отметить, что больше половины студентов (около 90%), принявших участие в стажировке, остаются работать в компании. Мы считаем это отличным показателем.

Сегодня у нас четыре стажировочные площадки, которые находятся в Санкт-Петербурге, Томске, Уфе и Пензе, что, несомненно, дает возможность региональным представительствам расширяться, не испытывая кадрового голода.

### С УВЕРЕННОСТЬЮ СМОТРИМ ВПЕРЕД!

— Готовы ли вы поделиться информацией о своих коммерческих успехах? С какими результатами вы завершаете 30-летний цикл?

— Несмотря на то что пандемия коронавируса, под знаком которого прошел 2020 г., серьезно ударила по экономике всей страны, на бизнес компании это не оказало негативного влияния. Наоборот, наши продажи выросли и

составили более 7 млрд рублей для группы компаний.

Такое положение дел вполне объяснимо: экстренный переход наших заказчиков на удаленный режим работ позволил продемонстрировать все преимущества наших продуктов по обеспечению безопасного удаленного подключения к корпоративным информационным системам.

Для многих оказалось неожиданно, что в наших продуктах, предназначенных для удаленного доступа, уже заложены сценарии безопасного подключения, в этой части мы не делали ничего нового.

Кроме этого, видя трудности, которые испытывают наши заказчики и партнеры за время карантина мы безвозмездно передали более 1 млн временных лицензий на наши продукты, обеспечив их необходимым техническим сопровождением. Это позволило им оперативно перейти на «удаленку», не испытывая никаких проблем, связанных с выделением средств на закупку решений для обеспечения безопасного удаленного доступа.

В конечном итоге эти факторы оказали положительное влияние на продажи. Прогнозы на 2021 г. также обнадеживают, будем надеяться, что тенденция роста сохранится и в дальнейшем. Мы же планируем активно работать над улучшением существующих продуктов и выводом на рынок новых разработок. Подводя итог, хочу сказать, что мы с оптимизмом и надеждой смотрим вперед — на следующие 30 лет.

— **Спасибо! Желаем успехов!**

*Вопросы задавал Валерий Куликов*

### ИНФОТЕКС СЕГОДНЯ — ЭТО:

♦ один из лидеров российского рынка в области «гражданской» криптографии, удовлетворяющий почти все потребности бизнеса и государственных органов в средствах защиты информации;

♦ поставщик средств сетевой безопасности, в частности криптошлюзов, межсетевых экранов нового поколения, программно-аппаратных комплексов (ПАК), способных конкурировать с зарубежными аналогами, удовлетворяя при этом требования регуляторов;

♦ надежный партнер крупных коммерческих и государственных компаний в сфере организации доверенного электронного документооборота;

♦ поставщик продуктов для построения SOC;

♦ центр развития перспективных направлений в сфере ИБ, в том числе систем квантовой криптографической связи;

♦ поставщик услуг в сфере дополнительного профессионального образования и повышения квалификации в области информационной и кибербезопасности.