Security Engineering: часть 16. Что то кончается, что то начинается

Published: 02.07.2026 09:50 | Updated: 08.07.2026 10:57

Эпоха системной безопасности: как изменилась профессия инженера по защите информации

Мы находимся в середине грандиозных перемен в том, как осуществляется безопасность. За последнее десятилетие ландшафт защиты информации трансформировался до неузнаваемости, и чтобы понимать будущее, необходимо осознать, как изменились роль специалистов, технологии и сама философия безопасности.

От «архипелага» к единой системе и смена ролей

Десять лет назад руководитель службы безопасности крупной компании, как правило, был отставным военным или полицейским. Компьютерная безопасность считалась незначительной узкой специализацией, которую поручали компьютерному отделу. Физическая охрана и замки оставались в ведении этого же руководителя. Однако в перспективе ближайших десяти лет руководителем станет системный инженер. Физическую безопасность (замки и охрану) передадут на аутсорсинг специализированным компаниям по управлению объектами.
Раньше технологии безопасности представляли собой «архипелаг» взаимно подозрительных островов: криптологи, специалисты по защите ОС, разработчики охранной сигнализации и химики, создававшие краски для банкнот. Каждый считал, что мир заканчивается на его берегу. Сегодня эти острова соединяются мостами. Практики понимают, что необходим системный

взгляд. Химик, создающий краски для банкнот, должен разбираться в цифровых водяных знаках, а криптолог не может ограничиваться лишь конфиденциальностью каналов связи.

Переосмысление самой сути безопасности

Десять лет назад информационная безопасность определялась триадой: «конфиденциальность, целостность и доступность». Сегодня во многих приложениях эти приоритеты меняются местами. Инженерия безопасности теперь заключается в том, чтобы системы оставались предсказуемо надежными перед лицом злонамеренных действий, ошибок, случайностей и даже принуждения.
Поскольку атаки смещаются от «железа» к людям, человеческие, институциональные и экономические факторы становятся столь же важными, как и технические. Цели защиты становятся более тонкими и близкими к бизнес-приложениям: конфиденциальность, безопасность и подотчетность. При этом часто возникают конфликты между целями, например, когда одной стороне требуется подотчетность, а другой — возможность отрицания (deniability).

Крах старых иллюзий и сложность как главный враг

Раньше лучшие продукты безопасности разрабатывались для правительств в условиях секретности и производились оборонными подрядчиками по системе «затраты плюс». Сегодня коммерческое использование многократно превышает государственное. В будущем гражданские ведомства будут использовать стандартные коммерческие технологии, а военные — готовые решения с полок магазинов (COTS). Изменилась и государственная политика: если раньше она была посвящена поддержанию эффективности огромных сетей коммуникационной разведки времен Холодной войны, то к 2000 году контроль за криптографией стал неактуальным и был отменен. На первый план вышли конфиденциальность, DRM, защита прав потребителей и электронное голосование.
Главным техническим вызовом сегодня стали системная интеграция и гарантия (assurance). Десять лет назад обитатели «островов» были полны уверенности в своих продуктах: криптологи верили, что шифры невозможно взломать, производители смарт-карт утверждали, что их чипы физически невозможно зондировать, создатели голограмм заявляли, что для подделки требуется докторская степень и оборудование на $20 млн, банкиры считали, что их банкоматы не могут ошибочно списать средства, адепты многоуровневой безопасности (MLS) полагали, что их подход решит все проблемы, а оценки по

«Общим критериям» (Common Criteria) всегда честны и компетентны.
Сегодня эти привычные certainties (уверенности) испарились. Безопасность стала частью более широкой проблемы надежности (dependability). Мы создаем всё лучшие инструменты, которые позволяют забираться всё выше на гору сложности, но в итоге мы всё равно с нее падаем. Доля крупных сложных системных проектов, терпящих неудачу, осталась на уровне 1970-х годов, но масштабы катастроф сегодня несоизмеримо больше.
Сложность — это реальный враг безопасности. Различие между «внешними» и «внутренними» нарушителями, которое раньше упрощало задачу, стремительно исчезает. Если раньше защита опиралась на несколько крупных идей и точные формулировки, то теперь она представляет собой разнообразное, неточное и эвристическое знание. Жизненный цикл систем изменился: если раньше это был закрытый проект с четкими рамками, то теперь системы эволюционируют и накапливают функции без ограничений.

Экономика, корпоративная память и регуляторные провалы

Изменения в природе работы также играют свою роль. Раньше главный внутренний аудитор банка помнил все мошенничества за последние 30 лет и не позволял IT-отделу повторять старые ошибки. Новая корпоративная культура с ее текучкой кадров и «перманентной революцией» (как это называл Мао) уничтожила корпоративную память.
Экономика гарантирует, что небезопасные системы будут создаваться, а ответственность — перекладываться на других. Правительства пытаются не отставать, но они слишком медлительны и подвержены влиянию лоббистов. Мы сталкиваемся с чередой регуляторных провалов.

Портрет инженера по безопасности XXI века

Защита информации в компьютерных системах больше не является научной дисциплиной — это инженерия. Инженер по безопасности XXI века несет ответственность за системы, которые постоянно эволюционируют и сталкиваются с меняющимся спектром угроз.
В его распоряжении большой набор инструментов. Ему необходимо постоянно поддерживать технический уровень: понимать новейшие атаки, уметь использовать новые инструменты и следить за юридическими и политическими тенденциями. Ему требуется прочный интеллектуальный фундамент: криптология, управление доступом, потоки информации, сети и обнаружение сигналов. Он также должен понимать основы менеджмента: как работают счета, принципы финансов и бизнес-процессы клиента.

Но самое главное — это способность управлять технологиями и эффективно участвовать в процессе эволюции системы для удовлетворения меняющихся бизнес-потребностей. Умение общаться с бизнес-людьми, а не только с другими инженерами, станет жизненно важным навыком, а опыт будет иметь огромное значение. Вряд ли такой специалист когда-либо останется без работы или будет скучать.

Долг перед обществом: борьба со страхом

Наконец, нельзя игнорировать политический и социальный контекст. Бурный рост индустриально-охранного комплекса после событий 11 сентября стал шрамом на мире и на нашей профессии. Наш долг — помочь ему зажить. Авторский путь решения этой проблемы лежит через исследования в области инженерии и экономики безопасности, чтобы понимать, что работает в реальном мире, а не только в лаборатории. Распространение знаний — ключевой фактор. Экономический рост и образование также помогают: именно бедных и необразованных легче всего запугать с помощью нагнетания страха (как со стороны западных лидеров, так и со стороны бен Ладена).
По крайней мере, в странах с образованным населением избиратели начали распознавать излишества «Войны с террором». Демократия является ключевым механизмом адаптации. Поэтому последний и, возможно, самый важный способ, которым инженеры по безопасности могут внести свой вклад, — это участие в политических дебатах. Чем активнее мы будем вовлекать людей, которые руководят дискуссиями о возникающих угрозах, тем быстрее наши общества смогут адаптироваться к ним.