Cleverics

Как ломаются сложные системы

Автор – Ричард Кук, MD.
Перевод – Роман Журавлёв, компания Cleverics.

На русском языке впервые опубликовано в ноябре 2009 года.

Cleverics (www.cleverics.ru) — компания, которая помогает применять возможности информационных технологий с пользой, рационально, с минимальными рисками. И с удовольствием. Основные направления деятельности Cleverics – построение и оптимизация ИТ-процессов, оценка и аудит управления ИТ, автоматизация ITSM-процессов, обучение руководителей и сотрудников ИТ.

1) Опасность – неотъемлемый атрибут сложных систем

Все интересные системы (транспорт, здравоохранение, энергетика…) естественно и неминуемо опасны по своей природе. На частоту опасных явлений в ряде случаев можно влиять, но процессы, входящие в состав этих систем, сами по себе являются источником неотвратимой опасности. И именно присутствие этой опасности приводит к созданию многочисленных средств защиты, столь характерных для этих систем.

2) Сложные системы тщательно и успешно защищаются от сбоев

Чем опаснее возможные сбои, тем более сложной становится со временем система защиты от них. Системы защиты включают в себя как очевидные технические решения (резервирование, автоматизированные средства обеспечения техники безопасности и т. п.) и «человеческие» решения (обучение, тренировки), так и разнообразные организационные, институциональные, нормативные способы защиты (политики и процедуры, сертификацию, правила…). Все они фокусируются на построении линий обороны, обычно направляющих работу системы в безаварийное русло.

3) Катастрофа подразумевает множество сбоев – одиночных нарушений недостаточно

Оборонительные сооружения работают. Работа систем, как правило, успешна. Заметные глобальные сбои возникают, когда несколько мелких, безобидных в сущности сбоев объединяются, создавая возможность глобальной системной аварии. Каждый из этих сбоев необходим для создания аварии, но только вместе они добиваются результата. Иными словами, возможностей для возникновения системных аварий гораздо больше, чем проявившихся аварий. Большая часть этих возможностей блокируется на ранней стадии развития созданными для этого средствами защиты. Большинство дошедших до уровня эксплуатации блокируется специалистами.

4) Сложные системы содержат постоянно меняющуюся комбинацию скрытых сбоев

Сложность рассматриваемых систем делает невозможной работу без множественных внутренних ошибок. Поскольку каждая из них неспособна привести к аварии, на операционном уровне они рассматриваются как несущественные. Устранение всех этих ошибок признается экономически нерациональным; кроме того, проактивная оценка их влияния на возможность возникновения системной аварии затруднена. Набор ошибок в составе системы постоянно меняется вместе со сменой технологий, организации работ, а также вследствие усилий по их устранению.

5) Сложные системы работают в режиме ограниченной производительности

Из сказанного выше следует, что сложные системы всегда работают как поврежденные системы. Система продолжает функционировать, поскольку содержит множество дополнительных средств обеспечения устойчивости, а также поскольку люди заставляют ее работать, несмотря на наличие множества ошибок. В ходе разбора случившихся аварий почти всегда отмечается, что в системе накоплена история «прото-сбоев», которые чуть не стали причиной аварии. Утверждение, что эти ситуации должны были быть выявлены заранее, обычно основано на упрощенном понимании работы систем. В то время как эта ра-

бота – и результирующая производительность системы – есть непрерывно меняющееся сочетание сбоев и восстановлений компонентов (организационных, человеческих, технических).

6) Катастрофа всегда рядом

Сложные системы склонны к катастрофам. Работающие с ними специалисты почти всегда находятся в непосредственной близости – как в пространстве, так и во времени – от возможной аварии: она может случиться в любой момент и почти в любом месте. Способность к катастрофе – фамильное свойство сложных систем. Устранить это свойство невозможно, оно присуще самой природе сложных систем.

7) Попытки найти «корневую причину» аварии – в корне ошибочны

Поскольку системные аварии происходят как следствие сочетания множества ошибок, не существует единственной «причины аварии». Всегда действует множество факторов, несущественных поодиночке, но совместно ведущих к аварии. Поэтому невозможно определить «корневую причину» аварии. Расследования, направленные на выявление такой причины, основываются не на техническом понимании природы сбоя, но лишь на социальной потребности возложения на кого-то или что-то определенной вины за случившееся1.

8) Необъективность ретроспективной оценки работы специалистов

Знание последствий заставляет нас преувеличивать очевидность приведших к нему событий для специалистов. Это означает, что анализ работы людей, проводимый ex post facto, дает неточные результаты. Знание случившегося впоследствии мешает проводящему анализ объективно оценить поведение специалистов в прошлом. Ему кажется, что люди «должны были знать», что те или иные события «неминуемо» привели бы к аварии2. Необъективность ретроспективного анализа остается основным препятствием для расследования катастроф, в особенности – при экспертной оценке работы персонала.

9) Люди играют двойную роль: создают сбои и защищают от них

Специалисты управляют системой для того, чтобы получить продукт, ради которого она создана, и предотвратить аварии. Это неизбежная динамическая характеристика работы системы – постоянный поиск баланса между спросом на продукцию и возможностью начала аварии. Сторонние наблюдатели редко осознают двойственность этой роли. Во время стабильной работы основной является производственная роль; при возникновении сбоев – защитная. В обоих случаях сторонний наблюдатель не осознает постоянной и одновременной вовлеченности специалистов в исполнение обеих ролей.

10) Все действия специалистов – авантюры

После аварий, когда случившиеся сбои выглядят единственно возможным следствием прошлых событий, действия специалистов воспринимаются как ошибки или как намеренное грубое пренебрежение этими событиями. На самом деле все их действия – это рискованные авантюры, попытки угадать будущие неопределенные события. Степень неопределенности может меняться от случая к случаю. То, что это именно угадывание, становится ясным вскоре после аварии – последующий разбор полетов собственно и показывает, что они не угадали.

Но то, что успешная работа систем – тоже результат угадывания, не является столь же очевидным и общепринятым.

11) Работа на переднем крае устраняет колебания

Организации колеблются, часто ненамеренно, между достижением целей, рациональным использованием ресурсов, экономией и снижением затрат и контролем рисков аварий. Все эти противоречия устраняются за счет работы специалистов на переднем крае систем. После аварии действия специалистов могут трактоваться как «ошибки» или «отклонения», но такие оценки находятся под влиянием ретроспективной необъективности и не учитывают другие движущие силы, в особенности – требования к производительности.

12) Специалисты – адаптивный элемент сложных систем

Специалисты и линейные руководители первого уровня активно адаптируют системы для получения максимальной производительности при минимуме аварий. Эта адаптация часто производится несистемно, от случая к случаю. Вот некоторые примеры такой адаптации:

1. Реструктуризация системы для снижения влияния уязвимых элементов.

2. Концентрация ресурсов в областях, где ожидается наивысший спрос.

3. Подготовка путей восстановления на случай ожидаемых и неожиданных сбоев.

4. Внедрение средств раннего обнаружения отклонений в производительности системы с целью соответствующей коррекции производства или активации других методов повышения устойчивости.

13) Уровень экспертизы специалистов в сложных системах постоянно меняется

Сложные системы требуют серьезной экспертизы для управления и эксплуатации. Эта экспертиза меняется при изменении технологий, но она также меняется и при смене сотрудников. В любом случае, обучение и обновление знаний – необходимая часть работы системы. Следовательно, в любой момент времени всякая система включает в себя специалистов с разным уровнем экспертизы. Серьезные сложности, связанные с экспертизой, возникают (1) при необходимости использования редкой экспертизы для наиболее сложных или важных производственных задач и (2) при необходимости развивать экспертизу для использования в будущем.

14) Изменения создают новые виды сбоев

Низкий уровень видимых нарушений в надежных системах может стимулировать изменения, в особенности – применение новых технологий, для устранения несущественных, но частых сбоев. Эти изменения могут привести к появлению возможностей для новых сбоев – редких, но существенных. Когда новые технологии используются для устранения известных мелких ошибок или повышения производительности, они часто становятся источником масштабных, катастрофических аварий. Нередко эти новые аварии имеют даже большее влияние, чем те, что были предотвращены внедрением новых технологий. Новые виды сбоев трудно опознать заранее; внимание уделяется в основном предполагаемым преимуществам от внедрения изменения. Поскольку новые крупные аварии возникают нечасто, до их первого проявления может пройти несколько изменений системы, что затрудняет опре-

деление связи аварий с новыми технологиями.

15) Поиск «причины» снижает эффективность мер защиты от будущих сбоев

Пост-аварийные меры в отношении «человеческих ошибок» основаны на пресечении или предотвращении действий, которые могут стать причиной аварии. Такие действия в отношении крайнего звена цепи мало способствуют снижению вероятности аварии в будущем. На самом деле вероятность повторения в точности такой же аварии и без того исчезающее мала, так как сочетание лежащих в ее основе многочисленных ошибок постоянно меняется. Вместо повышения уровня безопасности меры, принимаемые по результатам расследования аварий, только повышают сложность системы. Вместе с ней повышается вероятное число скрытых ошибок и затрудняется работа по их отслеживанию и устранению.

16) Безопасность – характеристика системы, а не ее компонентов

Безопасность – это общее свойство системы; она не может быть сведена к личности, устройству или отделу. Ее нельзя купить или произвести; она неотделима от других компонентов системы. Это значит, что безопасностью нельзя управлять как ресурсом. Состояние безопасности любой системы всегда динамично, непрерывные изменения системы ведут к непрерывным изменениям угроз и управления ими.

17) Люди непрерывно создают безопасность

Бесперебойная работа – это результат деятельности людей, удерживающих систему в приемлемых рамках производительности. По большей части эта деятельность – часть обычной ежедневной деятельности и внешне очень проста. Но поскольку работа системы никогда не бывает полностью свободной от ошибок, именно способность специалистов адаптироваться к меняющимся условиям обеспечивает безопасность системы в каждый момент времени. Эта способность часто предполагает лишь способность выбрать один из стандартных вариантов поведения; однако в отдельных случаях она требует создания новых комбинаций или даже принципиально новых подходов к работе системы.

18) Работа без сбоев требует опыта работы со сбоями

Выявление опасности и успешное управление системой с целью сохранить производительность в приемлемых рамках требуют тесного контакта с ошибками. Добиться высокой производительности удается в тех системах, где специалисты могут почувствовать грань, когда работа системы становится менее стабильной, менее предсказуемой или не может быть уверенно диагностирована. В системах, которые по определению опасны, это значит – вычислять и контролировать опасности так, чтобы общая производительность системы оставалась в согласованных рамках. Улучшения безопасности зависят от наличия у специалистов масштабируемого подхода к угрозам и от их способности прогнозировать влияние корректирующих действий на положение системы относительно границы между максимальной производительностью и неуправляемым разгоном.

Сноски:

1. Исследования в области антропологии указывают на социальное значение понятия «причина» (ср. Goldman L (1993), The Culture of Coincidence: accident and absolute liability in Huli, New York: Clarendon Press; а также Tasca L (1990), The Social Construction of Human Error, неопубликованная докторская диссертация, кафедра социологии Университета Стони Брук).

2. Это характерно не только для медицины или техники, но является общим свойством осознания людьми событий, случившихся в прошлом.

Краткий реферат других работ автора:

- «Природа сбоев»
- «Как развиваются аварии»
- «Как определяются причины сбоев»
- «Итоги нового взгляда на безопасность пациентов»

Другие материалы:

- Cook, Render, Woods (2000). «Gaps in the continuity of care and progress on patient safety». British Medical Journal 320: 791–4.
- Cook (1999). «A Brief Look at the New Look in error, safety, and failure of complex systems». (Chicago: CtL).
- Woods & Cook (1999). «Perspectives on Human Error: Hindsight Biases and Local Rationality. In Durso, Nickerson, et al., eds., Handbook of Applied Cognition». (New York: Wiley) pp. 141–171.
- Woods & Cook (1998). «Characteristics of Patient Safety: Five Principles that Underlie Productive Work». (Chicago: CtL)
- Cook & Woods (1994), «Operating at the Sharp End: The Complexity of Human Error», in MS Bogner, ed., Human Error in Medicine, Hillsdale, NJ; pp. 255–310.
- Woods, Johannesen, Cook, & Sarter (1994), «Behind Human Error: Cognition, Computers and Hindsight», Wright Patterson AFB: CSERIAC.
- Cook, Woods, & Miller (1998), «A Tale of Two Stories: Contrasting Views of Patient Safety», Chicago, IL: NPSF.