
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
1930
МЭИ

конференция РусКрипто

Механизм создания системы доверия к социально значимым общественным информационным системам

Минзов Анатолий Степанович, доктор технических наук, профессор кафедры БИТ НИУ «МЭИ»

Невский Александр Юрьевич, кандидат технических наук, заведующий кафедрой БИТ НИУ МЭИ

Баронов Олег Рюрикович, кандидат технических наук, доцент кафедры безопасности БИТ НИУ МЭИ

22.03.2023

Что такое социально значимые информационные системы?

1. Официальные сайты государственных органов и органов местного самоуправления в сети "Интернет».
2. Официальные сайты государственных внебюджетных фондов Российской Федерации в сети "Интернет».
3. Порталы государственных и муниципальных услуг.
4. Иные сайты в сети "Интернет", информационные системы и программы для электронных вычислительных машин, имеющие социальную значимость.

Постановление Правительства РФ от 29 декабря 2021 г. N 2531 "Об утверждении Правил ведения перечня отечественных социально значимых информационных ресурсов"

Что мы понимаем под термином «доверие» к социально значимым ИС?

- Для ***социально значимых информационных систем*** (СЗИС) термин «доверие» воспринимается сегодня как ***многокомпонентная функция,*** конечные значения которой существенно зависят от концепции ИТ-проекта, способов его реализации и архитектуры системы его безопасности.
- Общественно социальная степень доверия к ИТ-проектам СЗИС во многом определяется медийной частью и уровнем организационно-технической реализаций технологий обеспечения доверия к ИТ-проекту.

$$D = f(d_m) \oplus f(d_t),$$

где $f(d_m)$ - функция плотности распределения доверия субъекта к ИТ – проекту за счет использования СМИ и других медийных средств;

$f(d_t)$ - функция оценки уровня доверия субъекта к проекту ИТ на этапах проектирования и производства проекта ИТ, его архитектуры безопасности, испытания и поддержания его безопасного состояния.

Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (выписка) приказ ФСТЭК №76 от 2.06.2020.

Как обеспечивается доверие $f(d_t)$ к ИТ-проектам ?

1. Доверие к ИТ-проектам в концепции стандарта ГОСТ 15408 (часть 3) это «***основа для уверенности в том, что продукт ИТ отвечает целям безопасности***».
2. В этом стандарте определен и механизм обеспечения доверия, как «***бездоказательное утверждение, предшествующий аналогичный или специфический опыт***», а также с использованием активного исследования ИТ-продукта для определения его свойств безопасности.
3. Требования доверия представляются в виде структуры: ***класс-семейство-компонент-элемент***.
4. Основные принципы этого стандарта состоят в том, что следует ***четко сформулировать угрозы безопасности*** (Класс APE, семейство SPD), ***положения политики безопасности организации*** и ***продемонстрировать достаточность предложенных мер безопасности***.
5. Основной способ достижения доверия основан на проведении его оценки (всего 6 оценочных уровней доверия). Методы оценки основаны на ***анализе процессов, требований к ним, верификации доказательств, независимом функциональное тестирование, анализе уязвимостей и тестирование на проникновение***.
6. Доверие к техническим средства ИТ-проектов обеспечивается транзитивно через посредников (сертифицированных технических средств, удостоверяющих центров и т.д.).
7. Модель оценки угроз основана на нарушении механизмов доступности, целостности и конфиденциальности. (Банк данных угроз) ФСТЭК). ***Достаточно ли это ?***

ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности»

О моделях угроз, относящихся непосредственно к доверию ИТ-проекта СЗИС

1. В банке данных угроз ФСТЭК представлены всего 4 прямые угрозы по доверию:

   УБИ. 021: Угроза злоупотребления доверием потребителей облачных услуг.

   УБИ. 128: Угроза подмены доверенного пользователя.

   УБИ. 134: Угроза потери доверия к поставщику облачных услуг.

   УБИ. 217: Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения.

2. Все остальные угрозы относятся к конфиденциальности, целостности и/или доступности информации, что является необходимым условием доверия к ИТ-проекту. Эти угрозы также косвенно влияют на оценочный уровень доверия.

3. Однако этого недостаточно. Часть угроз может быть обнаружена в технологических и функциональных процессах обработки информации. а также в процессах измерения параметров, их обработки и передачи. Вопросы достоверности и актуальности информации в базах данных СЗИС также практически не рассматриваются с позиций обеспечения безопасности.

Банк данных угроз ФСТЭК https://bdu.fstec.ru

Какие решения в архитектуре безопасности могут привести к снижению доверия к СЗИС ?

1. Наличие процессов, целостность которых не контролируется.
2. Наличие каналов, которые могут контролироваться злоумышленниками и искажать информацию.
3. Недостоверные источники информации.
4. Некорректные оценки ОУД.
5. Применение несертифицированных технических средств защиты.
6. Применение несертифицированных криптографических алгоритмов и технологий (блокчейн, гомоморфного шифрования и т.д.).
7. Неконтролируемые средства виртуализации.
8. Неконтролируемые действия сотрудников при работе в СЗИС.
9. Нарушения принципа изменения уровня конфиденциальности по мере обобщения информации в СЗИС.
10. Нарушение принципа непрерывности работы СЗИС с позиций информационной безопасности.
11. Нарушение принципа анонимности, если это условие работы пользователей с СЗИС.
12. Размещение СЗИС на неконтролируемых государством порталах (информационных ресурсах).
13. Отсутствие общественного контроля за проектированием, тестированием, внедрением, аттестацией и эксплуатацией СЗИС.
14. Отсутствие документации на ИТ-проект СЗИС.
15. Отсутствие контроля за внесением изменений в систему.

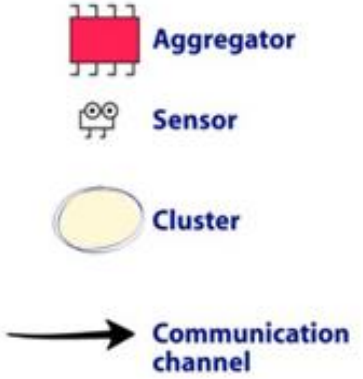
Концепция архитектуры безопасности ZTA

- Сущность концепции "Zero Trust Architecture" (ZTA, Архитектура нулевого доверия) заключается в реализации основного принципа отношения к любой информационной системе, как к системе ***с нулевым доверием***.
- Это предполагает создание такой архитектуры информационной безопасности, которая построена на принципе ***постоянного и полного контроля достоверности источников информации, всех субъектов доступа (пользователи, приложения, устройства) и объектов доступа (корпоративная сеть, интернет, приложения, объекты ввода-вывода информации и другие компоненты информационных систем).***
- Это не исключает использование существующей концепции транзитивного доверия третьей стороны (сертификаты на технические средства защиты информации, SSL, аттестованные объекты информатизации, удостоверяющих центров.
- Сложность подобно организованных информационных систем в несколько раз превышает сложность обычных систем.

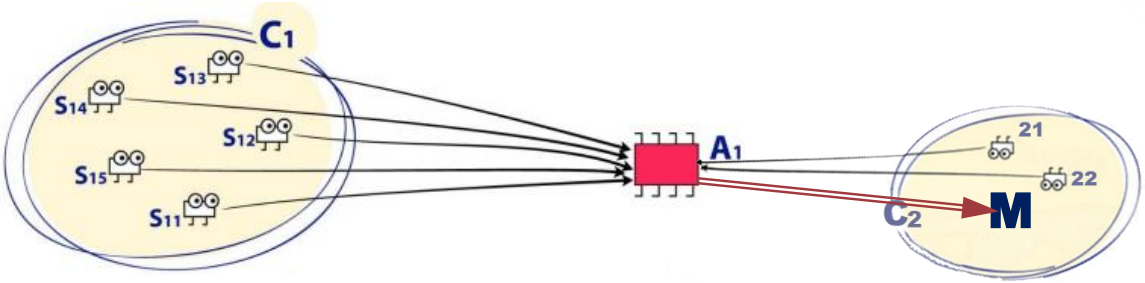
Scott Rose, Oliver Borchert, Stu Mitchell, Sean Connelly NIST Special Publication 800-207 “Zero Trust Architecture” URL https://doi.org/10.6028/NIST.SP.800-207, August 2020

Пример реализации концепции ZTA на модели КФС

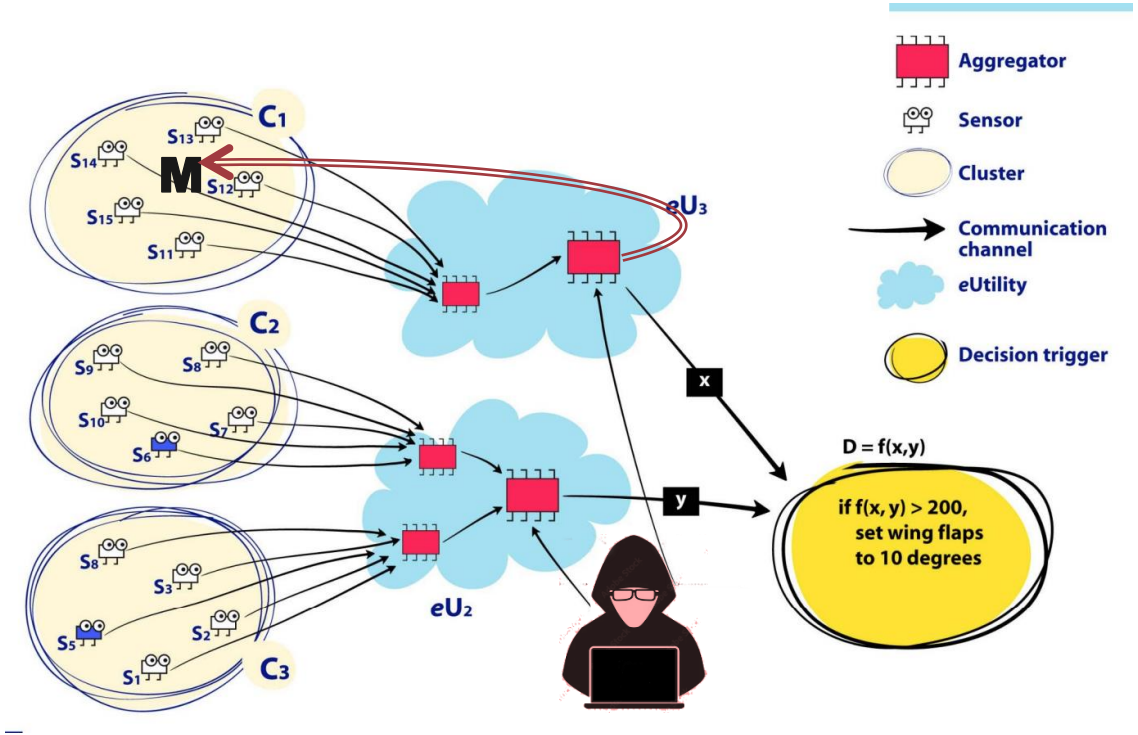
a)



b)

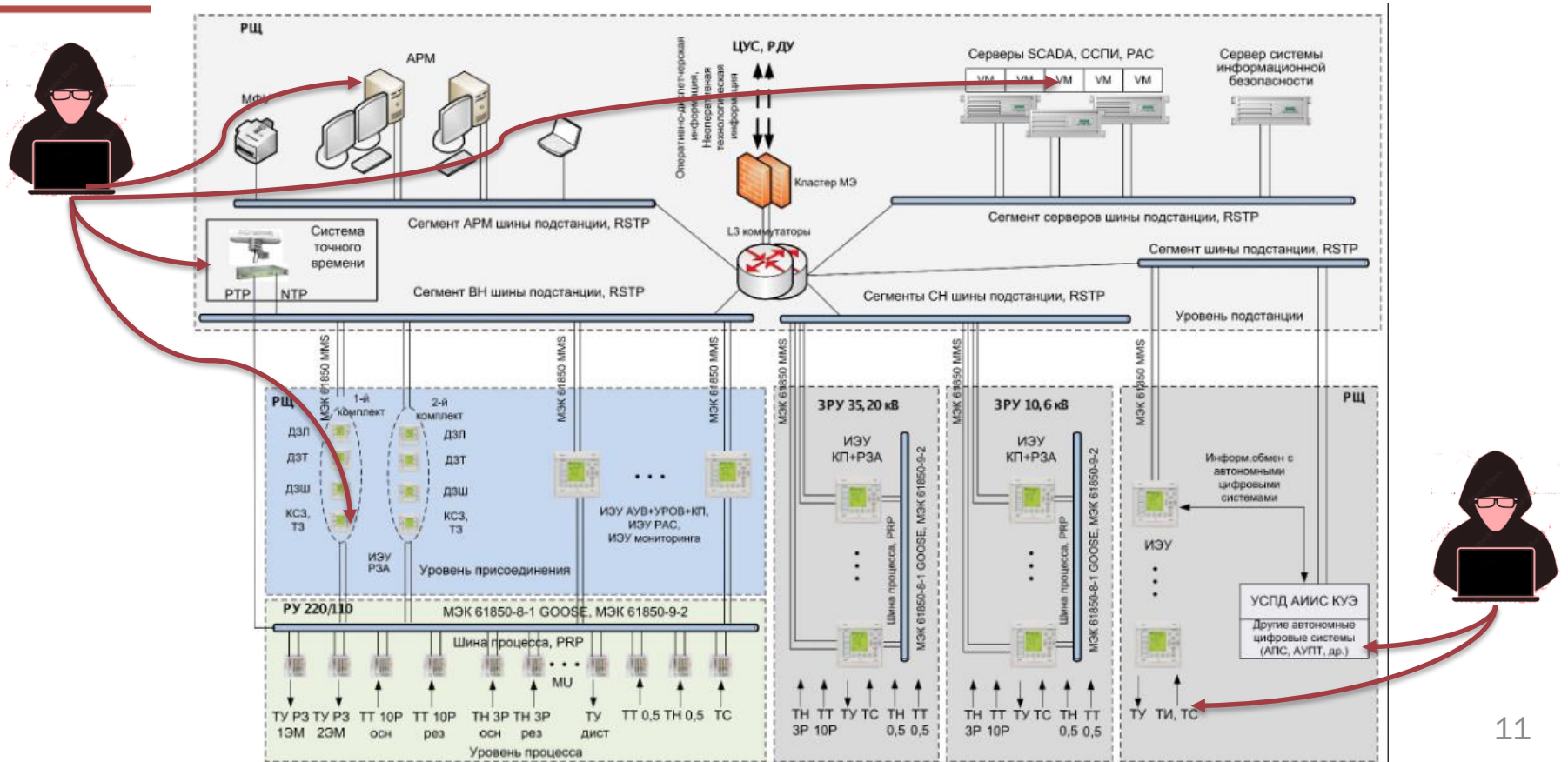


Более сложная реализация архитектуры безопасности КФС



Jeffrey Voas NIST Special Publication 800-183 Networks of 'Things' http://dx.doi.org/10.6028/NIST.SP.800-183

Структурная схема современной АСУТП



Механизмы доверия в других ИТ проектах

- Исследования, проведенные во ВЦИОМ Российской Федерации показали, что около 60% избирателей допускают умышленные манипуляции и мошенничество в системе ДЭГ, при этом около половины из них не верят в техническую возможность сохранения тайны голосования.
- Если говорить о социально-демографическом портрете тех, кто не одобряет обеспечение возможности дистанционного голосования на выборах, то, как правило, это мужчины (55%), респонденты в возрасте от 35 до 44 лет (53%) или же старше 60 лет (53%), а также оценивающие свое материальное положение как плохое или очень плохое (55%).
- Результаты этих исследований говорят о том, что существующая система доверия строится, в основном, на технологиях коммуникаций, СМИ и PR. Создание системы доверия к проекту ДЭГ на основе технических средств сегодня проводится на косвенных и неубедительных логических аргументациях.

Модель угроз доверия в системе ДЭГ

1	Нарушение тайны голосования.
2	Невозможность контроля избирателем результата своего голосования после подсчета голосов.
3	Голосование под давлением.
4	Голосование другим лицом.
	Передача права голосования другому лицу.
6	Передача права голоса не проголосовавшему избирателя без его ведома до момента закрытия системы голосования.
7	Фальсификация результатов голосования в момент голосования.
8	Фальсификация результатов голосования в момент подсчета голосов.
9	Фальсификация результатов при выводе их на устройства отображения.
10	Неактуальность реестра избирателей.
11	Фальсификация в момент двойного голосования (очное и электронное).
12	Передача результатов голосования конкретных избирателей заинтересованным лицам и организациям.
13	Невозможность контроля за действиями участников избирательного процесса и лицами, сопровождающими систему ДЭГ.
14	Фальсификация выборов за счет применения несертифицированных криптографических алгоритмов.
15	Фальсификация выборов путем применения несертифицированных технологий блокчейн и смарт-контрактов.
16	Отсутствие системы, методик и процедур тестирования ИС ДЭГ.
17	Недостаточный уровень принимаемых мер защиты из-за недооценки ОУД применяемых технических средств в подсистеме подсчета голосов ДЭГ.

Условия «абсолютного» доверия к ИТ-проекту СЗИС

Пусть x_i – элемент информационной структуры ИТ-проекта ($x_i \in X$), в котором происходит обработка информации в соответствии политикой безопасности. Определим x_i как $x_i = \{a_i, t_i, m_i, d_i\}$,

где a_i — функция обработки информации;

t_i — угроза и оценка меры ее влияния на уровень доверия;

m_i — мера по снижению угрозы;

d_i — метрика измерения уровня доверия ($d_i \in D: 0 \leq d_i \geq 1$).

Оценка уровня доверия всего ИТ-проекта $f(d_t)$ может быть представлена в следующем виде:

$a)$ $\forall x_i, (m \in M), (M \neq \emptyset), (t_i \in \emptyset) \rightarrow (d \cong 1)$ «абсолютное» доверие $f(d_t)$.

$b)$ $\forall x_i, (M \neq \emptyset), (\exists t_i: t_i \in \emptyset, m_i \in M) \rightarrow (d = min\{d_i\})$ реальное доверие $f(d_t)$.

Выражения *a)* и *b)* действительны при условии выполнения требований к классу (APE) семейства (SPD).

Заключение

DOUGLAS MCGREGOR: THEORY X AND THEORY Y 1960у.

Первый, кто предложил рассматривать систему управления в органи-зации как недоверен-ную среду

1. В настоящее время социально значимые общественные системы требуют повышенного внимания к доверию к ним общества и системы государственного и муниципального управления.
2. Доверие к СЗИС рассматривается как многокомпонентная функция, значения которой определяются медийной частью и уровнем организационно-технической реализации технологий обеспечения доверия к ИТ-проекту.
3. Существующие механизмы определения оценочного уровня доверия не гарантируют полного доверия к ИТ-проекту, так как не учитывают полный комплект угроз, относящихся к доверию СЗИС.
4. Концепция архитектуры информационной безопасности ZTA позволяет создавать ИТ-проекты с уровнем доверия к ним превышающие существующие уровни доверия к общественно значимым ИС. Эта концепция не противоречит «Общим критериям», а лишь уточняет модель и архитектуру безопасности объекта оценки.
5. В технических СЗИС такой подход потребует изменения концепций проектирования и модернизации SCADA – систем путем включения в их состав компонентов решающих типовые задачи информационной безопасности.

Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (выписка) приказ ФСТЭК №76 от 2.06.2020.

Спасибо за внимание !

Минзов Анатолий Степанович, доктор технических наук, профессор кафедры БИТ НИУ «МЭИ» (MinzovAS@mpei.ru)

Невский Александр Юрьевич, кандидат технических наук, заведующий кафедрой БИТ НИУ МЭИ

Баронов Олег Рюрикович, кандидат технических наук, доцент кафедры безопасности БИТ НИУ МЭИ