УДК 621.039.68 DOI: http://doi.org/10.25728/pu.2019.3.7

СИНТЕЗ АРХИТЕКТУРЫ КИБЕРБЕЗОПАСНОСТИ ДЛЯ СИСТЕМ УПРАВЛЕНИЯ АТОМНЫХ ЭЛЕКТРОСТАНЦИЙ

В.Г. Промыслов, К.В. Семенков, А.С. Шумов

Аннотация. Представлена комплексная модель кибербезопасности АСУТП. Предложен формальный метод классификации активов по уровням кибербезопасности с применением аппарата теории графов и алгоритмов кластеризации. Предложен метод синтеза архитектуры кибербезопасности систем и рассмотрена его применимость для иерархических систем. Представлен пример синтеза архитектуры кибербезопасности для подсистемы АСУТП атомной электростанции в соотвествии с политикой кибербезопасности МАГАТЭ и МЭК.

Ключевые слова: кибербезопасность, АСУТП, атомная электростанция, архитектура кибербезопасности, классификация, кластеризация, граф безопасности, модель «take-grant».

ВВЕДЕНИЕ

Безопасность системообразующих инфраструктурных объектов, к которым относятся и атомные электростанции (АЭС) — важный компонент безопасности общества и государства. На АЭС цифровая АСУТП выполняет как функции безопасности, так и функции нормальной эксплуатации [1]. Проблема обеспечения безопасности АСУТП АЭС (далее для краткости аббревиатуру АЭС будем опускать) комплексна и связана с обеспечением промышленной (энергетической, ядерной и радиационной, функциональной) безопасности [2], а из-за высокой степени централизации управления объектом на основе компьютеризированных систем — и с обеспечением информационной и кибербезопасности [3]. В международной практике для выделения кибербезопасности из информационной безопасности принята модель МАГАТЭ [4].

Процесс управления кибербезопасностью АСУТП в общем случае можно представить в виде последовательности выполнения следующих шагов [3]:

— собственник АЭС, в соответствии с требованиями в рамках программы информационной безопасности, определяет политики и процедуры безопасности для критически важной информации, нарушение доступности, целостности или конфиденциальности которой может привести к нарушению штатного режима функционирования АСУТП [4];

— в соответствии с выбранным уровнем описания системы (например, подсистема, процесс и др.) собственник идентифицирует и выделяет критически важные информационные активы, т. е. любые цифровые объекты АСУТП, которые могут влиять на кибербезопасность самой системы или объекта управления;

— собственник идентифицирует функциональность активов в разрезе обработки, хранения и передачи информации в цифровой форме

— по результатам оценок риска на системном уровне проводится классификация/категоризация активов, т. е. назначаются уровни кибербезопасности для активов АСУТП;

— в соответствии с уровнем кибербезопасности назначаются требования к мерам защиты;

— определяется архитектура безопасности АСУТП, в том числе правила разграничения доступа.

Перечислим существенные для обеспечения и анализа кибербезопасности системы свойства АСУТП.

- Система строится по иерархическому принципу, иерархия существует как на уровне архитектуры системы (наличие подсистем), так и на

уровне архитектуры кибербезопасности. Для обеспечения эффективной защиты и минимизации набора применяемых мер осуществляется группировка активов по уровням кибербезопасности. Этот процесс неотделим от задачи категоризации/классификации активов. Объединение активов на уровне архитектуры системы приводит к появлению комплексных активов, которые принадлежат к другому уровню иерархии. Например, актив на уровне компьютера может рассматриваться как объединение активов: процессы, файлы и т. д.

- Основное внимание уделяется сохранению доступности и целостности информации, данные свойства доминируют над принципом сохранения конфиденциальности информации [5].
- Существует устоявшаяся классификация активов по ядерной безопасности, которая может служить базой при классификации активов по кибербезопасности [1].
- Для сохранения целостности основные потоки информации идут от активов с высшим уровнем кибербезопасности к активу с низким уровнем, однако существует технологическая необходимость передавать информацию в обратном направлении. Фактически, с некоторыми исключениями, реализуется модель Биба [6].

Можно заключить, что комплексная задача синтеза архитектуры кибербезопасности АСУТП разбивается на несколько частных задач, таких как категоризация/классификация активов, назначение барьерных мер, согласование информационных связей и др., и сейчас они решаются преимущественно экспертным методом. Как и у любого субъективного метода, результаты решения зависят от квалификации экспертов, нет эталона для сравнения результатов работы разных групп экспертов и пр. Делаются попытки формализации задачи классификации активов, например, представлен подход к оценке кибербезопасности АСУТП на базе методов структурно-логического анализа надежности и безопасности с применением вероятностных моделей [7], рассмотрен метод анализа кибербезопасности на основе теории графов и дискреционной модели доступа [8]. Однако в целом аспект обеспечения кибербезопасности АСУТП до сих пор является нерешенным вопросом в структуре обеспечения безопасности АСУТП, особенно на стадии проектирования и согласования функциональных требований и решений (мер) кибербезопасности.

Рассмотрим задачу — создать комплексную модель кибербезопасности, применимую для АСУТП, которая позволила бы не только описать архитектуру кибербезопасности АСУТП, но и классифицировать активы, определить механизм для синтеза архитектуры безопасности системы, основанной на заданных функциональных связях между активами, свойствах системы и принятой политике безопасности.

1. КОМПОНЕНТЫ МОДЕЛИ КИБЕРБЕЗОПАСНОСТИ

В качестве компонентов комплексной модели кибербезопасности мы воспользовались дискретной моделью безопасности [9] для задания информационных связей и решеточной моделью доступа, задающей политику безопасности в системе и предложенной в работе [10].

Определение 1. Комплексная модель кибербезопасности АСУТП — это совокупность компонентов $ICM = \langle SLM, DM, R\rangle$, где DM (*data model*) описывает модель обмена информации между активами, компонент SLM (*security level model*) задает общие правила доступа к информации между уровнями кибербезопасности системы, а набор операторов R задает правила соответствия между активами и уровнями. ♦

Далее рассмотрим компоненты модели подробнее.

1.1. Модель правил доступа к информации

Модель правил доступа определена как совокупность множества классов (уровней кибербезопасности) и отношений между ними и правил, регулирующих отнесение актива к уровню $SLM = \langle SC, \oplus, \rightarrow, \nrightarrow\rangle$, где SC — конечное линейно-упорядоченное множество уровней кибербезопасности, состоящее из N_{SC} элементов; $\rightarrow$ — отношение, определенное на паре уровней безопасности ($L_1 \rightarrow L_2$ означает, что информация в простом виде от уровня L_1 может передаваться уровню L_2, где подстрочный индекс задает порядковый номер уровня); $\nrightarrow$ — отношение, определенное на паре уровней безопасности ($L_2 \nrightarrow L_1$ означает, что информация от уровня L_2 может передаваться уровню L_1 в безопасном виде); $\oplus$ — оператор группировки (он будет рассмотрен в § 2).

Определим, что передача информации в безопасном виде означает, что на пути передачи информации установлены определенные барьеры безопасности. Если на пути передачи информации барьеров между активами не установлено, то будем говорить о простой передаче информации.

В работе [10] показано, что элементы SC, $\oplus$, $\rightarrow \vee \nrightarrow$ формируют решетку уровней кибербезопасности. Удобно задавать решетку доступа в виде направленного ациклического графа $G_{SLM} = \langle SC, E\rangle$, $E = \{e_1, e_2, ..., e_n\} \cup \{\rightarrow, \nrightarrow\}$.

1.2. Модель обмена информацией

Компонент модели DM описывается дискретной моделью безопасности: $DM = \langle G^*, OP\rangle$, где $G^* = \langle\{G_i | i = 1, N\}\rangle$ — все возможные состояния системы, которые описываются графом доступа G_i с вершинами $A = \{A_i\}$, заданными активами, а ребра задают бинарное отношение между парой активов, описывающее направление передачи информации между активами, которые необходимы для обеспечения заданной функциональности системы, OP — множество операций преобразования графа доступа, введенных в рамках модели (будем далее называть их допустимыми) $G_1 = \langle A, \{\mapsto, \rightarrow\}\rangle$.

По аналогии с п. 1.1, будем говорить, что информация между активами передается безопасно, если на пути передачи информации между активами установлены определенные барьеры безопасности. Мы не конкретизируем вид этих барьеров, так как он зависит от реализации моделируемой системы. Если же на пути передачи информации барьеры между активами не установлены, то будем говорить о простой передаче информации.

Ребра в графе доступа относятся к одному из двух типов: простая передача информации $\mapsto$, безопасная передача информации $\rightarrow$. Запись $a \mapsto b$ означает, что информация от актива a передается активу b простым способом. Запись $a \rightarrow b$ означает, что информация от актива a передается активу b безопасным способом.

Мы ввели разные обозначения для операторов передачи информации между уровнями и между активами, чтобы подчеркнуть разную природу отношений передачи: активы — это реальные физические объекты, тогда как уровни — это абстрактное представление объединения и ранжирования активов.

Определение 2. Будем называть операции чтения ($\overset{r}{\mapsto}$) и записи ($\overset{w}{\mapsto}$) антисимметричными, если $a \overset{w/r}{\mapsto} b \not\Rightarrow b \overset{r/w}{\mapsto} a$, иными словами, если операция записи/чтения из a в b не приводит к возможности чтения/записи из b в a.

Определение 3. Назовем передачу информации безопасной, если из отношения $a \rightarrow b \not\Rightarrow a \mapsto b$, т. е. передача информации для $L^a < L^b$, где $L_x = R(x)$, не нарушает целостности/конфиденциальности актива b. ♦

Примером безопасной передачи может служить замена записи информации активом a в актив b на операцию чтения активом b из актива a, при условии, что приняты меры, обеспечивающие нарушение симметричности операций r и w.

Сформулируем полезное свойство, что из $a \rightarrow b \not\Rightarrow a \mapsto b$, и наоборот, из $a \mapsto b \Rightarrow a \rightarrow b$, $L^a > L^b$, и $a \mapsto b \not\Rightarrow a \rightarrow b$, $L^a \le L^b$.

1.3. Операторы отображения моделей *SLM и DM*

Для более ясного восприятия предположим, что множество графов доступа G^* содержит граф G_i, который является, как минимум, слабо связным. Введем на вершинах G^* порядковую функцию:

$$P(G^*) = \{X: x_1, ..., x_M\}, \quad M \le M_A,$$

где M_A — количество активов, Далее введем оператор R, выполняющий преобразование:

$$R(P(G^*)) = \Lambda(l, D).$$

Здесь $\Lambda(l, D)$ — ориентированный граф с M вершинами, которые соответствуют точкам множества $\{X\}$. Обозначим через $A_k \subset A$ и $A_m \subset A$ множества всех активов, которые переходят в вершины l_k и l_m графа Λ соответственно. Тогда правила построения ребер графа $\Lambda(l, D)$ запишутся следующим образом:

а) если $\exists a_i \in A_k$ и $a_j \in A_m$: $(a_i a_j) \in \mapsto(A)$ и $P(a_i) \ne P(a_j)$, то $(l_k l_m) \in \rightarrow$;

б) если $\forall a_i \in A_k$ и $a_j \in A_m$: $k \ne m$, $(a_i a_j) \notin \varnothing$ выполняется условие $(a_i a_j) \in \rightarrow$, то ребро $(l_k l_m)$ графа Λ существует, причем $(l_k l_m) \in \twoheadrightarrow$.

Если граф G^* распадается на несколько областей связности, то

$$R(P(G^*)) = \cup_i R(P(G^{*i})),$$

где G^{*i} — отдельные области связности.

Итак, введение порядковой функции $P(G^*)$ и оператора R означает:

- ранжирование и группировку активов по уровням значимости;
- установление соответствия между информационными связями активов и отношениями доступа между уровнями.

2. СИНТЕЗ АРХИТЕКТУРЫ КИБЕРБЕЗОПАСНОСТИ АСУТП

Под термином «синтез архитектуры кибербезопасности» будем понимать процесс приведения модели DM в соответствие с моделью SLM.

Дадим определение кибербезопасной АСУТП в рамках данной модели.

Определение 4. Система, которая описывается моделью ICM, является кибербезопасной, если любая последовательность допустимых операций (OP) над активами в ней не может привести к нарушению потоком информации отношения $\rightarrow$ или $\twoheadrightarrow$. Про такие системы будем говорить, что у них модель DM согласуется с моделью SLM (соответствует модели SLM). ♦

В § 1 мы наложили на число уровней M, задаваемых порядковой функцией $P(G^*)$, единственное ограничение: $M \le M_A$. Введем оператор группировки уровней $\oplus$, который стягивает граф $\Lambda(l, D)$ в граф $\Lambda'(l', D')$, число вершин в котором не превосходит N_{SC}.

Ранг (уровень) L новой вершины l', полученной объединением вершин $l_1, l_2, ..., l_n$, задается выражением $L = L^{l_1} \oplus L^{l_2} \oplus L^{l_3} \ldots \oplus L^{l_n} = \inf(\{L^{l_1}, L^{l_2}, L^{l_3}, ..., L^{l_n}\})$.

Ребра графа $\Lambda'(l', D')$ формируются по правилу:

а) если все $l_k \overset{\oplus}{\to} l'_q$ и $l_m \overset{\oplus}{\to} l'_p$, где $l'_q \ne l'_p$ и $(l_k l_m) \notin \varnothing$, удовлетворяют условию $(l_k l_m) \in \nrightarrow$, то ребро $(l'_p, l'_q) \notin \varnothing$ и $(l'_p, l'_q) \notin \nrightarrow$;

б) если найдутся такие $l_k \overset{\oplus}{\to} l'_q$ и $l_m \overset{\oplus}{\to} l'_p$, где $l'_q \ne l'_p$ и $(l_k, l_m) \notin \varnothing$, для которых $(l_k l_m) \in \to$, то ребро $(l'_p, l'_q) \notin \varnothing$ и $(l'_p, l'_q) \notin \to$.

Пусть имеются некоторые две модели *SLM* и *DM*. Оператор $R(P(G^*))$ осуществляет отображение (сюръекцию) вершин графа G^* на множество вершин графа $\Lambda(l, D)$.

Достаточное условие того, что модель *DM* соответствует модели *SLM*, формулируется следующим образом. *Если граф, полученный отображением $R(P(G^*))$, после применения оператора группировки $\oplus$ изоморфен какому-либо минору G^m_{SLM} графа G_{SLM}, т. е. $\Lambda(l, D) \overset{\oplus}{\to} \Lambda'(l', D') \simeq G^m_{SLM}$, то модель DM соответствует модели SLM.*

Доказательство следует из определений функции P и операторов $R(P(G^*))$ и $\oplus$, а также из определения 4.

На практике достаточное условие соответствует утверждению: *если имеется спроектированная система, то после присвоения активам уровней кибербезопасности правила доступа к информации между разными уровнями не должны нарушаться.*

Заметим, что на отображение $R(P(G^*))$ и граф G_{SLM} могут быть наложены дополнительные условия. Например, в рамках обеспечения ядерной безопасности исключают прямую передачу любой информации непосредственно между активами, чей класс ядерной безопасности отличается друг от друга больше чем на единицу [1]; аналогичный принцип применяется и для обмена информации между активами, классифицированными по уровням кибербезопасности, что накладывает ограничения на смежные активы в графе G^* [5].

3. МЕТОД КАТЕГОРИРОВАНИЯ АКТИВОВ И СИНТЕЗА АРХИТЕКТУРЫ КИБЕРБЕЗОПАСНОСТИ

Дадим практическую методику синтеза архитектуры кибербезопасности, основанную на изложенных выше принципах.

Порядковая функция P описывает процесс упорядочения активов, а оператор R расставляет упорядоченные активы по уровням кибербезопасности и выстраивает информационные связи между уровнями.

Мы предлагаем рассмотреть задачу классификации активов как типичную задачу кластеризации [10], т. е. выявления групп объектов, к которым применимы одинаковые критерии. Представленный подход полностью учитывает сложившуюся практику классификации активов по кибербезопасности для АЭС, изложенную в профильных документах МАГАТЭ и МЭК [4, 5].

В кластерном анализе под кластером обычно понимается часть данных, в типичном случае — подмножество объектов, характеризуемых подмножеством переменных, которое выделяется из всего множества наличием некоторой однородности элементов.

Задачу кластеризации можно разделить на четыре подзадачи [12]:

— выбор представления исходных данных для анализа;

— определение вида искомой кластерной структуры;

— выбор критерия оценки кластерной структуры;

— выбор метода построения кластерной структуры.

Рассмотрим каждую из подзадач более детально.

3.1. Типы исходных данных и выбор представления данных для анализа

Для выбора представления данных необходимо идентифицировать активы, определить значения признаков на активах, шкалы измерений. Для задания отношений между признаками и активами предлагается воспользоваться таблицей вида «актив — признак». Для описания признаков задействуются различные типы шкал: ранговая (отражающая ранг), количественная (применяющаяся к количественно измеримым характеристикам), номинальная (применяющаяся к качественным характеристикам).

Число признаков может быть произвольным, но в данной работе для наглядности мы ограничились тремя признаками.

- Класс объекта по ядерной безопасности (от 1 до 3), которому принадлежит актив. Класс ядерной безопасности, присвоенный системе, в зна-

чительной мере определяет ценность системы, так как с ним однозначно связан ущерб от выхода системы из строя. Для задания признака применяется ранговая шкала, приведенная к количественному виду порядковой функцией $R_1(x) = \{1, 2, 3, 4\}$ (для 1-, 2- и 3-го классов и 4 для неклассифицируемых активов соответственно).

- Функциональное свойство или функциональные свойства актива (актив рассматривается в виде серого ящика, обладающего некоторыми внутренними свойствами). Для дальнейшей обработки признак следует привести к количественному виду с помощью порядковой функции: $R_2(x) = \{0, 1, 2, 3, ...\}$.
- Информационные свойства актива — характеристики, отражающие информационные связи актива с другими активами.

Информационные свойства актива в части кибербезопасности в значительной мере определяются силой воздействия на систему при нарушении конфиденциальности, целостности и доступности информации, ассоциированной с активом. Классическим подходом для оценки информационных свойств является экспертное ранжирование по фиксированным уровням [14]. Мы рассмотрим аналитический метод для приведения данного признака к количественному виду.

Пусть информационные свойства S актива $a_j \in A$ системы есть некоторая характеристика, зависящая от трех параметров: $S(a_j) = S(C(a_j), I(a_j), T(a_j))$, — где C — конфиденциальность, I — целостность, T — доступность. В дальнейшем, там, где нет необходимости, нотация a_j будет опускаться. В рамках нашей упрощенной модели положим, что $T = T(a_j, t)$ — функция времени и характеристик актива, а $C = C(a_j)$ и $I = I(a_j)$ — функции только характеристик актива. Далее пренебрежем зависимостью кибербезопасности от времени — это разумное допущение на верхнем уровне анализа архитектуры кибербезопасности системы, когда фактически игнорируются динамическое поведение системы. Тогда кибербезопасность можно представить как $S = S(C, I, T)$, $T = \text{const}$.

В информационной безопасности, описываемой дискретной моделью, допустимо считать, что целостность и конфиденциальность не являются независимыми характеристиками (модели Биба и модель Белла — Ла Падулы [14]), а их можно выразить друг через друга.

Достаточно оценить лишь один параметр C или I и воспользоваться для оценки другого параметра моделью, описывающей их зависимость. Мы будем исследовать только свойство целостности, потому что, в соответствии с распространенным подходом [5], основное внимание в АСУТП уделяется сохранению целостности. Тогда

$$S_1(C, I) = S_1(C, I(C)) = S_1(C(I), I).$$

Таблицу признаков можно записать в виде, представленном в табл. 1.

Таблица 1

Признаки активов АСУТП с упрощенным разбиением по информационным свойствам
(в скобках поясняются используемые признаки)

Актив	Класс по ядерной безопасности	Характеристика актива	Информационные свойства актива
(Идентификатор)	(Класс актива в выбранной системе классификации)	(Функциональность активов в разрезе обработки, хранения и передачи информации)	(Характеристика связанности актива с другими активами)

3.2. Отношение порядка на графе безопасности

Из существования отношения порядка на подмножестве вершин (см. Приложение) следует, что на этом подмножестве мы можем ввести порядковую функцию $R(x)$. Значение порядковой функции для актива можно использовать как количественную характеристику информационных свойств актива: $S_1(C(I), I) \sim R_3(x)$.

Наша порядковая функция должна каким-то образом выделить наиболее «важные» активы, т. е. такие активы, которые, будучи скомпрометированы, значительно увеличат риск нарушения целостности системы. Для оценки предположим, что *более важным в смысле организации защиты считаем элемент системы, который передает информацию большему числу абонентов*. Тогда мы приходим к следующей порядковой функции графа безопасности: число исходящих из вершины ребер после транзитивного замыкания графа безопасности по выбранному отношению доступа. Такой подход аналогичен применению метрик цикломатической сложности (точек ветвления) для программного обеспечения при оценке его надежности, когда наиболее критичным модулем программы считается модуль с наивысшей цикломатической сложностью [15].

3.3. Перенормировка данных

После приведения всех признаков к численному виду каждому активу будет соответствовать вектор порядковых функций, задающих численное значение соответствующего признака для актива $\{R_1(x), ..., R_n(x)\}$, где индекс означает номер признака в таблице признаков (см. табл. 1). Такая таблица содержит данные с независимыми столб-

цами, и значения разных признаков, хоть и приведены в численном виде, часто несопоставимы, так как каждый признак, вообще говоря, имеет свою единицу измерения. Для приведения признаков к сопоставимому виду проводится перенормировка значений: у каждого признака изменяют точки отсчета и масштаб шкалы:

$$R'_{iv}(x) = (R_{iv}(x) - a_v)/b_v,$$

где $R_{iv}(x)$ обозначает исходную матрицу данных, $R'_{iv}(x)$ — перенормированную, i — активы, v — признаки. Параметр a_v задает сдвиг точки отсчета, а b_v — новый масштаб для каждого признака v. Для целей анализа данных, включая кластерный анализ, начало координат лучше всего помещать где-то в районе центра множества точек, представляющих признак для активов [12]. Что касается масштабирующих коэффициентов b_v, то их следует выбирать, исходя из идеи выравнивания относительных шкал признаков.

3.4. Критерии и метод кластеризации

Для разбиения активов на классы кибербезопасности мы предлагаем применить метод кластеризации разбиения с центроидами по методу k-средних [11]. Данный метод основывается на том интуитивном критерии, что объекты внутри кластеров должны быть близки друг к другу, а в разных кластерах — далеки друг от друга. Достоинство метода состоит в разбиении исходного множества на «выпуклые», хорошо интерпретируемые кластеры. Кластерная структура метода k-средних задается разбиением множества объектов S на K непересекающихся кластеров $S = \{S_1, S_2, ..., S_K\}$ с соответствующими центроидами $c = \{c_1, c_2, ..., c_K\}$. Минимизируемым критерием является сумма расстоянии $d(y_i, c_k)$ от объектов y_i до соответствующих центроидов c_k:

$$W(S, c) = \sum_{k=1}^{K} \sum_{y_i \in S_k} d(y_i, c_k),$$

где y_i — строка отнормированной матрицы $y_{iv} = R'_{iv}(x)$, полученной из таблицы «объект — признак», столбцы которой $v = 1, ..., V$ соответствуют признакам, а строки i — активам. Метрика $d(y_i, c_k)$ — это квадрат евклидова расстояния.

3.5. Присвоение уровней кибербезопасности и анализ согласованности моделей

Методы кластерного анализа позволяют разбить множество элементов на некоторое число групп по заданным критериям однородности элементов, однако они не задают отношений порядка между полученными кластерами.

В данной работе мы предлагаем выстроить отношение порядка между кластерами эмпирическим путем: в каждом из кластеров выбрать актив $A_i \in \{A_i\}$, которому в соответствии с критериями, специфическими для конкретной системы, присвоить некоторый уровень. Данный актив применяется как центр для кластера, содержащий активы данного уровня. При необходимости следует объединить отранжированные кластеры в уровни кибербезопасности. Данные операции (ранжирование и объединение подуровней в уровни) и задаются оператором $\oplus$ в модели *SLM*.

Итак, пусть мы разбили множество всех активов A на кластеры $\{S\}$, т. е. $A = S_1 \cup S_2 \cup ... \cup S_M$. Затем каждому кластеру присваивается ранг. Эти две операции соответствуют применению порядковой функции $P(G^*)$ на множестве активов кибербезопасности.

Затем к полученному упорядоченному множеству сгруппированных активов мы применяем оператор построения графа правил доступа $R(P(G^*))$, получив, таким образом, некоторый граф уровней кибербезопасности $\Lambda(l, D)$ на вычисленном нами разбиении. И, наконец, применив при необходимости оператор $\oplus$ к графу $\Lambda(l, D)$, мы получим ответ на вопрос о соответствии модели *DM* модели *SLM* в соответствии с достаточным условием, сформулированным в § 2.

4. О КАТЕГОРИЗАЦИИ В ИЕРАРХИЧЕСКИХ СИСТЕМАХ

Во всех проведенных выше рассуждениях не принималась в расчет иерархическая структура АСУТП. В реальной жизни почти всегда применяются системы, состоящие из подсистем (активы имеют внутреннюю структуру), которые, в свою очередь, включают в себя подсистемы и т. д. Если в исследуемой системе нет подсистем (активы атомарны), то предложенный метод дает полный формальный подход классификации активов по кибербезопасности.

Проведем рассуждения на примере системы с одним уровнем вложенности. Для иерархических систем с большей степенью вложенности можно воспользоваться методом индукции.

На этапе проектирования системы структура подсистем еще не проработана, но уже известен набор подсистем и информационные потоки между ними. Значит, можно построить граф безопасности, анализируемыми активами которого будут подсистемы, и применить предлагаемый нами формальный метод классификации подсистем по уровням безопасности. Тогда каждой подсистеме будет назначен какой-то класс безопасности.

Перед разработчиками подсистемы встает ряд вопросов. Если подсистеме назначен какой-то уро-

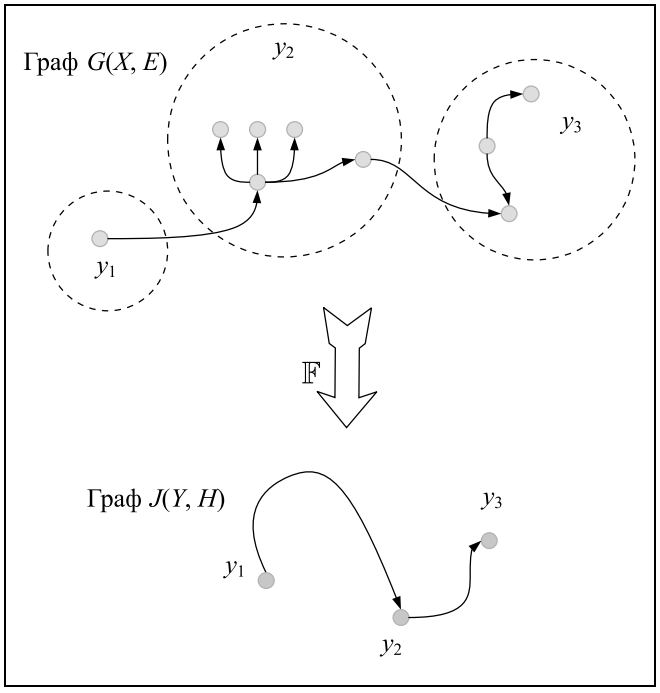

Рис. 1. Графы, описывающие информационную модель АСУТП со структурой подсистем и без нее (*вверху* и *внизу* соответственно)

вень кибербезопасности, то означает ли это, что все элементы подсистемы должны защищаться по данному классу? Например, если в подсистеме с высокими требованиями к безопасности есть вспомогательный элемент, который не оказывает влияния на функции системы, должен ли он быть защищен так же, как и основные элементы системы?

Рассмотрим два графа безопасности системы: $G(X, E)$, рис. 1, *вверху*, учитывает структуры подсистем, $J(Y, H)$, рис. 1, *внизу*, — нет. Очевидно, что J — это результат стягивания графа G: $J = \mathbb{F}(G)$, которое не является взаимно однозначным отображением. Формальный метод классификации, вообще говоря, даст различные результаты на графах $J(Y, H)$ и $G(X, E)$. Более того, так как порядковая функция графа строится на транзитивном замыкании графа безопасности, мы придем к парадоксальному выводу: разработчик отдельной подсистемы должен знать структуру всей системы и структуру связей в ней. Как мы видим, простое применение формального метода классификации на развернутом графе не дает практически применимых результатов.

Мы можем устранить данный парадокс, заметив, что, проведя на графе $J(Y, H)$ классификацию подсистем по уровням кибербезопасности, мы наложили на элементы подсистем в первоначальном графе $G(X, E)$ дополнительное условие: указали максимальный уровень кибербезопасности активов в подсистеме.

Мы предлагаем применить следующий алгоритм классификации систем с произвольным количеством уровней вложенности.

Первый шаг. Проектировщик системы строит граф безопасности, вершинами которого являются подсистемы, и проводит на нем классификацию активов. В результате каждой подсистеме назначается определенный класс безопасности. Между подсистемами одного класса могут устанавливаться опциональные барьеры; между подсистемами разных классов должны устанавливаться обязательные барьеры, причем, со стороны подсистемы с более высоким уровнем кибербезопасности. В рамках принятой модели безопасности установка барьера означает, что отношения вида «$\mapsto$» преобразуются в отношения вида «$\rightarrow$».

Второй шаг. Проектировщик каждой из подсистем строит граф безопасности своей подсистемы и проводит классификацию активов с наложенными дополнительными условиями: максимальный уровень кибербезопасности внутри подсистемы равен уровню кибербезопасности, назначенному всей подсистеме; множество активов подсистемы, расположенных на максимальном уровне, не пустое. После проведения классификации он также должен установить барьеры между группами активов: обязательные, если разделяемые группы относятся к разным классам по кибербезопасности, и опциональные, если группы относятся к одному классу по кибербезопасности.

Проектировщик подсистемы второго уровня (подсистемы внутри подсистемы) классифицирует активы своей подсистемы, описанную на втором шаге, и т. д.

5. ПРИМЕР СИНТЕЗА АРХИТЕКТУРЫ И ВЕРИФИКАЦИЯ РЕЗУЛЬТАТОВ

Рассмотрим как пример синтез архитектуры безопасности для модели безопасности RG 5.71 [16] (рис. 2). Данная модель, фактически с момента появления, стала стандартной для атомной отрасли в международном масштабе. Она с небольшими вариациями повторена в документах МАГАТЭ и МЭК [4, 5]. Для модели безопасности вводится 5 уровней компьютерной (кибер-) безопасности: самый высокий — 1, самый низкий — 5. Без ограничений поток данных разрешен с верхнего на более низкий уровень безопасности; передача

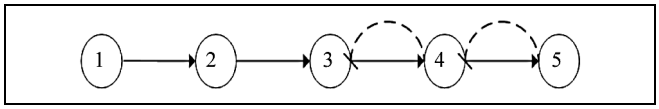

Рис. 2. Упрощенная информационная модель безопасности (штриховыми линиями показаны безопасные отношения)

данных с нижнего уровня на высший разрешена только для двух первых (самых низких) уровней кибербезопасности. Основная цель системы кибербезопасности, построенной по этой архитектуре, заключается в сохранении целостности данных и предотвращении модификации информации системами нижнего уровня кибербезопасности в системах верхнего уровня.

Поток данных от верхнего уровня к нижнему определяется наличием доступа на запись (w) от субъекта, принадлежащего более высокому уровню, к субъекту, находящемуся на низком уровне.

5.1. Классификация активов

Рассмотрим пример классификации активов S сегмента АСУТП, состоящего из нескольких подсистем (активов) ($a1$ — $a8$). Признаки системы сведены в таблицу признаков (табл. 2). В качестве функционального признака взята функция подсистемы, ранжированная от 1 до 3: управляющая подсистема, подсистема диагностики и мониторинга, вспомогательная подсистема. Граф безопасности системы, отображающий информационные связи в рамках модели дискреционной модели, представлен на рис. 3.

Для расчета признака «целостность» выполнено транзитивное замыкание графа по отношению w. Результат транзитивного замыкания приведен на рис. 4.

По итогам транзитивного замыкания рассчитываются значения введенной нами порядковой функции $R_3(x)$.

Таблица 2

Таблица признаков

Актив	Класс ядерной безопасности	Функциональный признак	Целостность
$a1$	1	1	7
$a2$	2		5
$a3$			
$a4$	3	3	4
$a5$		2	
$a6$			
$a7$		3	
$a8$	4	2	

Таблица 3

Разделение активов S по уровням кибербезопасности

Уровни Активы	$S1$ $a1$	$S2$ $a2$, $a3$	$S3$ $a4$, $a7$	$S4$ $a5$, $a6$	$S5$ $a8$

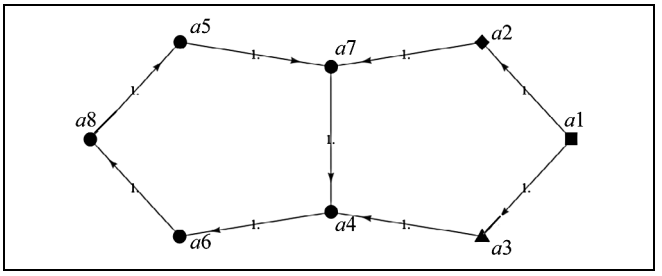

Рис. 3. Граф безопасности системы в рамках модели take-grant (группы сильно связанных активов выдедены формой вершин)

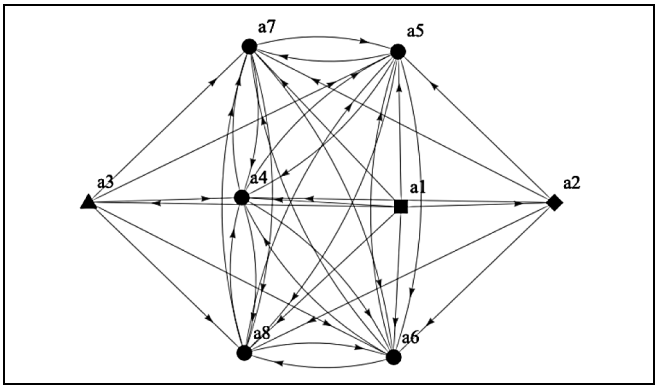

Рис. 4. Транзитивное замыкание для графа безопасности по отношению w

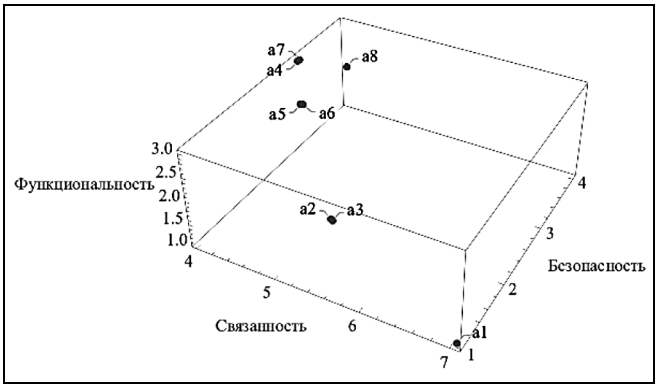

Рис. 5. Графическое отображение разделения активов по уровням кибербезопасности

В результате применения метода кластеризации было получено разделение всего множества активов на 5 непересекающихся подмножеств, где активы сгруппированы по сходству признаков. Графическое отображение этого разделения приведено на рис. 5, где оси на графике представляют собой шкалы соответствующего пространства признаков.

Искомое разделение активов по уровням кибербезопасности приведено в табл. 3.

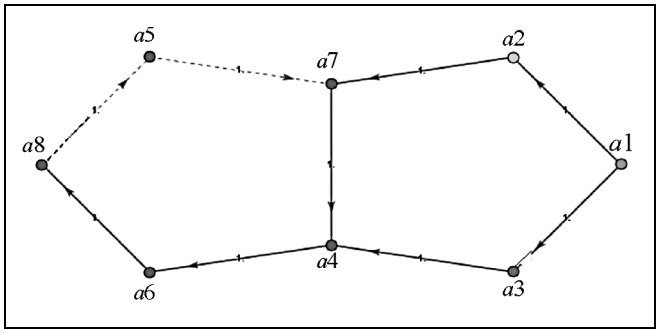

Рис. 6. Модифицированная архитектура сегмента АСУТП: безопасные связи показаны штриховыми линиями

5.2. Синтез архитектуры кибербезопасности

После классификации активов архитектура системы (см. рис. 3) должна быть приведена в соответствие с выбранной моделью безопасности (см. рис. 2). Можно видеть, что информационные потоки в архитектуре, представленной на рис. 3, в целом соответствуют требованиям архитектуры модели безопасности, однако для связи активов $a_8 \mapsto a_5$, $a5 \mapsto a7$ используются простые связи, что нарушает целостность активов $a7$, $a5$ со стороны активов, принадлежащих более низкому уровню кибербезопасности. Для исключения этого небезопасные связи должны быть трансформированы в безопасные. Для безопасного доступа активов с уровней 5 и 4 к субъектам на более высоких уровнях (4 и 3 соответственно), применяется безопасный антисимметричный доступ по чтению (r) (рис. 6).

ЗАКЛЮЧЕНИЕ

Вопросы обеспечения кибербезопасности до сих пор остаются непроработанными в структуре обеспечения безопасности АСУТП. Несмотря на существование норм и формальных правил (в виде набора мер) по обеспечению кибербезопасности, для АСУТП атомных электростанций отсутствуют методики согласования функциональных требований и решений по кибербезопасности. Представленная в данной работе комплексная модель кибербезопасности АСУТП состоит из двух основных компонентов, описывающих политику безопасности и информационную архитектуру системы соотвественно, и правил, задающих переход от одной модели к другой. В качестве первого компонента рассмотрена модель «решетка» уровней доступа *SLM*, которая задает общие правила доступа к информации между уровнями кибербезопасности системы В качестве второго компонента рассмотрена дискретная модель кибербезопасности *DM*, которая описывает обмен информации между активами. В рамках комплексной модели сформулированы правила перехода между моделями *DM* и *SLM*. Получено достаточное условие соответствия модели *DM* модели *SLM*.

Представлен пример синтеза архитектуры безопасности для АСУТП в соотвествии с политикой кибербезопасности RG5.71.

Отметим, что процесс согласования моделей (синтеза архитектуры) — это, вообще говоря, некорректная задача хотя бы потому, что активов обычно больше, чем уровней кибербезопасности, и системы, отличающиеся как числом активов, так и связями между ними, могут удовлетворять одной и той же модели прав доступа.

Есть основания полагать, что для практического применения важно сформулировать и доказать необходимые условия соответствия моделей для определенных типов систем. Если такие условия удастся получить, то для определенных типов систем можно получить шаблоны, которые позволят заданной модели уровней доступа сразу планировать связи между активами.

В рамках принятой модели уровней доступа предложен практический метод анализа безопасности системы и определения мест, в которых нужно установить барьеры для приведения системы к безопасному виду. Однако выбор способов реализации барьеров или, что то же самое, выбор и обоснование применения конкретных мер защиты в данной работе не рассмотрены.

Предложенный метод включает в себя способ категоризации активов по кибербезопасности, основанный на алгоритмах кластеризации множеств.

Отметим, что возможность практического применения предложенных методов для решения реальных задач зависит от средств моделирования, которыми располагает проектировщик. В работе использована облачная среда моделирования кибербезопасности [17].

ПРИЛОЖЕНИЕ

Применение модели take-grant для задания информационной модели АСУТП атомных электростанций

Представим информационную модель системы в виде графа (графа безопасности), отражающего физическую природу описываемых систем. Свойства такого графа приведены в табл. 4. Обозначим его как $G = G(X, E)$, где X — множество вершин, E — множество ребер.

Воспользуемся дискретной моделью распространения прав доступа, или моделью take-grant *(«брать-давать»)*

Таблица 4

Соответствие физических свойств моделируемой системы ее представлению в виде графа

Физическое свойство системы	Свойство графа $G(X, E)$
Действие имеет источник и потребителя	Направленность
Имеются разные типы активов безопасности (активные и пассивные)	Вершины могут быть разных типов
Имеются различные виды отношений между активами, например, чтение и запись	Ребра могут могут быть разных типов
Есть иерархия (по крайней мере, в отдельных подсистемах)	Существует отношение порядка (по крайней мере, на подмножестве вершин $\hat{X} \subset X \in G(X, E)$)
Наличие в системе элементов, которые не обмениваются информацией друг с другом	Граф не является тотальным (см. примечание)
Наличие в системе барьеров: шлюзов, брандмауэров, диодов данных	Граф не транзитивен, т. е. из отношения порядка $x_1 \le x_2$ между вершинами x_1 и x_2 не следует, что эти вершины соединены ребром $(x_1, x_2) \in E$
Реальность инженерных объектов	Граф конечен
Двойственность, симметричность отношений (например, отношений чтения и записи)	Граф может содержать циклы

Примечание. Напомним, что граф называется тотальным, если для любой пары вершин этого графа определено отношение порядка. В реальных системах могут быть элементы, не связанные друг с другом путями передачи информации, т. е. в графе не между всеми вершинами существует путь.

[18]. Отношения доступа между объектами и субъектами политики безопасности в этой модели описываются с помощью теории графов. Рассматриваемый в настоящей работе вариант модели take-grant основан на подходе, описанном в статье [8]. В рамках данной модели кибербезопасность представляется в виде графа безопасности G, где граф безопасности — это конечный помеченный ориентированный взвешенный мультиграф, описывающий состояние системы.

В графе выделяется два типа вершин: один соответствует субъекту, другой — объекту. Ребро, направленное из вершины A к вершине B, указывает на то, что вершина A имеет некоторое право (права) доступа к вершине B. Обычно стандартными считаются следующие права доступа: чтение (r) (*read*), запись (w) (*write*) (в части передачи информации), взятие (t) (*take*), выдача (g) (*grant*) (в части передачи прав). Отношения, связанные с передачей прав доступа $R = \{r_1, r_2, ..., r_n\} \cup \{t, g\}$, принято называть отношениями «де-юре», а $R = \{r_1, r_2, ..., r_n\} \cup \{w, r\}$ — отношениями «де-факто». Для отношений «де-факто» введен набор элементарных преобразований для описания передачи информации (*Post*, *Pass*, *Spy*, *Find*) и модификации графа — добавления и удаления вершин и ребер — (*Create*, *Delete*).

Начальный граф доступа G_0, задаваемый формальной моделью безопасности, может быть трансформирован последовательным применением элементарных правил в новый граф G' (трансформация обозначается как $G_0 \mapsto G'$). Кибербезопасность системы рассматривается с точки зрения возможности получения каким-либо субъектом прав доступа к определенному объекту (в начальном состоянии такие права отсутствуют) при определенной кооперации субъектов путем последовательного изменения состояния системы на основе выполнения элементарных команд. Рассматриваются условия санкционированного, т. е. законного получения прав доступа, и «похищения» прав доступа.

В работе [18] сформулированы условия, при которых субъект может осуществить доступ типа $e \in \{r, w, t, g\}$ к активу для указанного выше набора прав доступа и элементарных правил преобразования графа.

ЛИТЕРАТУРА

1. *Менгазетдинов Н.Э.*, *Бывайков М.Е.*, *Зуенков М.А.* и др. Комплекс работ по созданию первой управляющей системы верхнего блочного уровня АСУТП для АЭС «Бушер» на основе отечественных информационных технологий. — М.: ИПУ РАН, 2013. [*Mengazetdinov*, *N.E.*, *Poletykin*, *A.G.*, *Zuenkov*, *M.A.*, et al. Range of works on creation on the first upper block-level I&C system for NPP «Busher» on the base of domestic information technologies. — Moscow: ICS RAS, 2013. (In Russian)]
2. *ГОСТ Р* МЭК 61513—2011. Атомные станции. Системы контроля и управления, важные для безопасности. Общие требования. — URL: http://docs.cntd.ru/document/1200089290. [*IEC* 61513—2011. Nuclear power plants — Instrumentation and control important to safety — General requirements for systems. — URL: https://webstore.iec.ch/publication/5532]
3. *Бабаев Д.И.*, *Полетыкин А.Г.*, *Промыслов В.Г.*, *Тимофеев М.Ю.* Управление архитектурой кибербезопасности АСУТП атомных электростанций // Проблемы управления. — 2018. —

№ 3. — С. 47—55. [*Babaev*, *D.I.*, *Poletykin*, *A.G.*, *Promyslov*, *V.G.*, *Timofeev*, *M. Yu.* Control of cybersecurity architecture of nuclear power plants I&C // Control Sciences. — 2018. — No. 3. — P. 47—55. (In Russian)]
4. *Computer* security at nuclear facilities: reference manual: technical guidance // IAEA Nuclear Security Series. — 2011. — No. 17.
5. *IEC* 62645 (2014)/Cor.1 (2015). Атомные электростанции. Системы контроля и управления. Требования к программам обеспечения безопасности для компьютерных систем. — URL: https://webstore.iec.ch/publication/7311&preview=1. [*IEC* 62645(2014)/Cor.1(2015). Nuclear power plants — Instrumentation and control systems — Requirements for security programmes for computer-based systems. — URL: https://webstore.iec.ch/publication/7311&preview=1]
6. *Biba*, *K.J.* Integrity Considerations for Secure Computer Systems, MTR—3153. — The Mitre Corporation, June 1975.
7. *Харченко В.*, *Скляр В.*, *Брежнев Е.* Безопасность информационно-управляющих систем и инфраструктур. — Palmarium academic publishing, 2013. — 528 с. [*Harchenko, V.*, *Sklyar, V.*, *Brezhnev, E.* The Security of Information and Control Systems and Infrastructures. — Palmarium academic publishing, 2013. — 528 p. (In Russian)]
8. *Промыслов В.Г.*, *Полетыкин А.Г.* Формальная иерархическая модель безопасности верхнего уровня АСУТП АЭС // Ядерные измерительно-информационные технологии. — 2012. — Т. 4 (44). — С. 39—53. [*Promyslov*, *V.G.*, *Poletykin*, *A.G.* Formal Hierarchical Security Model of I&C Upper Level System of a Nuclear Power Plant // Nuclear Measurement and Information Technologies. — 2012. — Vol. 4 (44). — P. 39—53 (In Russian)]
9. *Девянин П.Н.* Модели безопасности компьютерных систем. — М.: Academia, 2005. — 144 с. [*Devyanin*, *P.N.* Security models for computed-based systems. — Moscow: Academia, 2005. — 144 p. (In Russian)]
10. *Denning*, *E.* A lattice model of secure information flow // Communications of the ACM. — 1976. — Vol. 19, iss. 5. — P. 236—243.
11. *Kaufman*, *L. and Rousseeuw*, *P.J.* Finding Groups in Data: An Introduction to Cluster Analysis. — NY: Wiley. — 1990. — 342 p.
12. *Mirkin*, *B.* Mathematical Classification and Clustering. — Dordrecht-Boston-London: Kluwer Academic Publishers, 1996. — 448 p.
13. *Wood*, *R.T.*, *Joseph III*, *R.A.*, *Korsah*, *K.*, et al. Classification Approach for Digital I&C Systems at U.S. Nuclear Power Plants. — Oak Ridge National Laboratory, 2012. — URL: https://www.nrc.gov/docs/ML1209/ML120970232.pdf.
14. *Bell*, *D.E.*, *La Padula*, *L.J.* Secure Computer System: Mathematical Foundations // MITRE Technical Report MTR—2547, vol. 1. — MITRE Corporation, Bedford, Mass., 1973.
15. *Harrison*, *W.A.* Applying Mccabe's complexity measure to multiple-exit programs. // Software: Practice and Experience. — 1984. — Vol. 14, iss. 10. — P. 1004—1007.
16. *U.S.* Nuclear regulatory commission. Research regulatory guide 5.71. Cyber security programs for nuclear facilities, January 2010.
17. *Omole* cybersecurity simulation toolkit. — URL: https://www.omole.ws.
18. *Bishop*, *M.* Computer Security: Art and Science. — Boston: Addison Wesley. — 2003. — 1136 p.

Статья представлена к публикации членом редколлегии В.В. Кульбой.

Поступила в редакцию 18.03.2019, после доработки 03.04.2019.
Принята к публикации 04.04.2019.

Промыслов Виталий Георгиевич — канд. физ.-мат. наук, ✉ v1925@mail.ru,

Семенков Кирилл Валерьевич — канд. физ.-мат. наук, ✉ semenkovk@mail.ru,

Шумов Александр Сергеевич — ✉ mau17@list.ru,

Институт проблем управления им. В.А. Трапезникова РАН, г. Москва.

SECURITY MODEL FOR INSTRUMENTATION AND CONTROL SYSTEMS FOR NUCLEAR POWER PLANTS

V.G. Promyslov[#], K.V. Semenkov, A.S. Shumov

V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia

[#]✉ v1925@mail.ru

Abstract. This paper presents a comprehensive cybersecurity model for process control systems. A formal method for classifying assets according to cybersecurity levels using the mapping system in the form of a graph and using clustering methods is proposed. A method for synthesizing the cybersecurity architecture of systems is proposed. The applicability of these methods for hierarchical systems is considered. An example of the synthesis of the security architecture for the subsystem of the NPP automated process control system is considered in accordance with the cyber security policy RG5.71. The Appendix describes the security graph in the take-grant model.

Keywords: cybersecurity, I&C, security architecture, NPP, nuclear power plant, classification, clustering, security graph, take-grant model.