УДК 004.654

ПОСТРОЕНИЕ ER-ДИАГРАММЫ ВЗАИМОСВЯЗИ ДАННЫХ О СОБЫТИЯХ И ИНЦИДЕНТАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФРАСТРУКТУРЕ ЦЕНТРОВ ИНФОРМАЦИОННОЙ ЗАЩИТЫ

Королев И.Д.,

д.т.н., профессор, профессор кафедры № 34

Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М.Штеменко,

Краснодар, Россия

Литвинов Е.С.

адъюнкт,

Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М.Штеменко,

Краснодар, Россия

Костров С.О.

старший оператор,

Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М.Штеменко,

Краснодар, Россия

Аннотация: Результат исследования вопросов информационной безопасности в работе центров информационной защиты показывает необходимость внедрения централизованной базы данных о событиях и инцидентах информационной безопасности в структуру этих центров. Цель работы – построение ER-диаграммы зависимости данных о событиях и инцидентах информационной безопасности, выявленных средствами центров информационной защиты. Для этого в работе произведено определение сущностей и связей данных о событиях и инцидентах информационной безопасности, позволяющее определить подход к построению

централизованного банка данных событий и инцидентов информационной безопасности. Полученный результат может быть использован для построения модели банка данных событий и инцидентов информационной безопасности.

Ключевые слова: информационная безопасность; SIEM-система; база данных; технические данные SIEM-системы, инцидент информационной безопасности, событие информационной безопасности.

BUILDING AN ER-DIAGRAM OF THE RELATIONSHIP OF DATA ON INFORMATION SECURITY EVENTS AND INCIDENTS IN THE INFRASTRUCTURE OF INFORMATION SECURITY CENTERS

Korolev I. D.,
doctor of technical Sciences, Professor, Professor of Department No. 34
Krasnodar higher military order of Zhukov and the October Revolution red banner school named after General of the army S. M. Shtemenko,
Krasnodar, Russia
Litvinov E. S.
adjunct,
Krasnodar higher military order of Zhukov and the October Revolution red banner school named after General of the army S. M. Shtemenko,
Krasnodar, Russia
Kostrov S. O.
senior operator,
Krasnodar higher military order of Zhukov and the October Revolution red banner school named after General of the army S. M. Shtemenko,
Krasnodar, Russia

Abstract: The result of the study of information security issues in the work of information security centers shows the need to implement a centralized database of information security events and incidents in the structure of these centers. The

purpose of the work is to build an ER diagram of the dependence of data on information security events and incidents detected by information security centers. To do this, the paper defines the entities and relationships of data about events and incidents of information security, which allows you to determine the approach to building a centralized database of events and incidents of information security. The obtained result can be used to build a model of a data Bank of information security events and incidents.

Keywords: information security; SIEM system; database; SIEM system technical data, information security incident, information security event.information security; SIEM system; database; SIEM system technical data, information security incident, information security event.

Поиск и обработка событий и инцидентов информационной безопасности – одна из основных задач, решаемых персоналом центров информационной защиты. В настоящее время основным инструментом решения этой проблемы является система управления инцидентами информационной безопасности (SIEM-система), которая позволяет собирать и обобщать, выявлять и генерировать данные о событиях и инцидентах информационной безопасности, а также обладает большим набором средств автоматизации процессов управления и координации действий персонала подразделений, обеспечивающих защиту информации [1].

SIEM – система способна получать данные от большого количества различных источников, которые могут формировать единый поток данных о событиях и инцидентах информационной безопасности [2]. Все эти источники представляют собой программные или программно-аппаратные решения, разрабатываемые различными фирмами и предприятиями. Вследствие этого данные о событиях и инцидентах информационной безопасности хранятся и транспортируются в различных видах и формах [3]. Разделение этого

информационного потока на отдельные данные позволило произвести группировку передаваемых данных на отдельные множества:

данных о контролируемых активах (A);

данных об установленном на узле программном обеспечении (B);

данных о сетевом взаимодействии активов (C);

данных о полученном контролируемыми активами (узлами сети) уроне при появления компьютерного инцидента (D);

данных о выявленных инцидентах информационной безопасности (E);

данных о состоянии аппаратной части контролируемых узлов (F);

данных о состояние локальной политики безопасности (G_l) и групповой политики безопасности (G_g);

данных о контролируемых узлах сети (H);

данных, определяющих место инцидента (события) в ранее выявленных цепях событий и инцидентов (I);

данных, вносимых в журнал регистрации компьютерных инцидентов (J);

данных о списке системных групп, в которые внесены пользователи (K);

данных, о персонале, задействованном в ликвидации последствий компьютерных атак (L);

данных о мерах, принимаемых для ликвидации последствий компьютерной атаки (M);

данных о событиях и инцидентах информационной безопасности, представленных в ненормализованном виде (N);

данных, содержащих эталонные значения конфигурационных файлов (O);

данных, содержащих рекомендации по ликвидации инцидентов информационной безопасности (P);

данных о состоянии средств защиты информации (R);

данных о выявленных событиях информационной безопасности (S);

данных о пользователях и их поведении (U).

Все эти данные имеют логические связи и представлены в формате графа на рисунке 1, имеющего следующий вид:

$$Sup = \langle A,B,C,C',D,E/S,F,G_l/G_g,H,I,J,K,L,M,N,O,P,R,U;\{[J,E/S]\}\cup\{[J,I]\}\cup$$
$$\cup\{[J,D]\}\cup\{[J,H]\}\cup\{[J,M]\}\cup\{[E/S,C]\}\cup\{[E/S,A]\}\cup\{[C,C']\}\cup\{[M,P]\}\cup\{[M,L]\}\cup$$
$$\cup\{[H,N]\}\cup\{[H,A]\}\cup\{[H,U]\}\cup\{[U,K]\}\cup\{[A,G_l/G_g]\}\cup\{[A,B]\}\cup\{[A,R]\}\cup\{[A,F]\}\cup$$
$$\cup\{[A,O]\}\rangle$$[4].

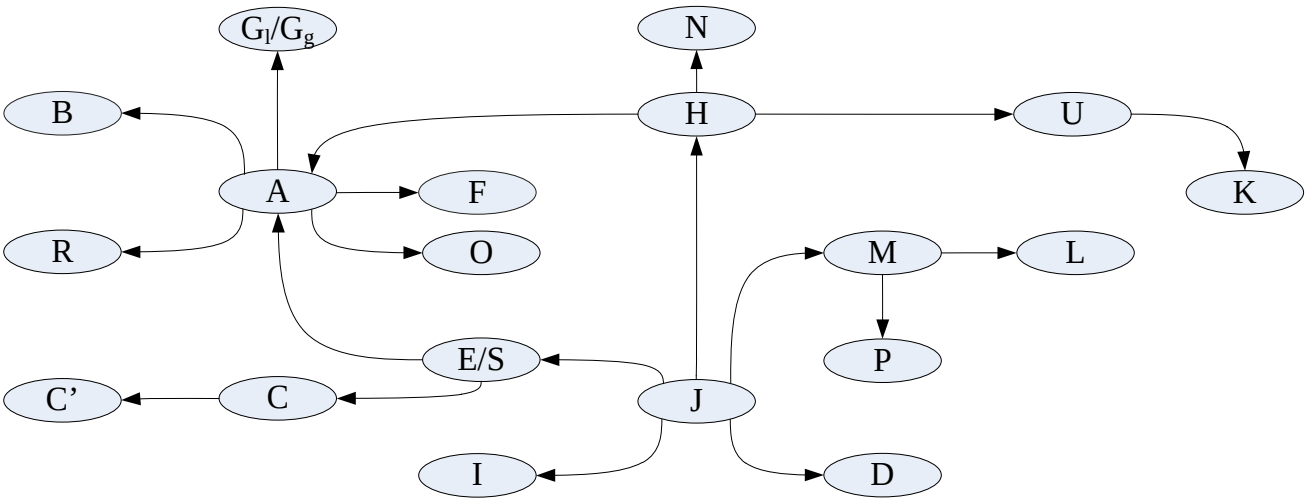


Рис.1 – Взаимосвязь данных о событиях и инцидентах информационной безопасности[1]

Граф зависимости данных о событиях и инцидентах информационной безопасности позволяет определить характеристики этих связей и построить более подробную структуру представления информации в виде ER-диаграммы (диаграммы определения сущностей и связей).

Для решения этой задачи необходимо произвести декомпозицию графа. Для этого необходимо произвести разделение графа на отдельные деревья. Очевидно, что при таком принципе деления графа будут получены подграфы, корневыми узлами которого станут узлы H, J, M, U, A, E/S, C.

На рисунке 2(а), представлен подграф Sub_H графа Sup, имеющий следующий вид:

$$Sub_H = \langle A,H,N,U;\{[H,N]\}\cup\{[H,A]\}\cup\{[H,U]\}\rangle.$$

[1] Разработано авторами

Подграф Sub_H отображает связь данных, описывающих контролируемый узел с данными:

о состоянии его активов;

о зарегистрированных на нем учетных записях;

о событиях и инцидентах информационной безопасности, представленных в ненормализованном виде.

При этом одной записи о контролируемом узле будет соответствовать:

несколько записей о зарегистрированных пользователях (на одном рабочем месте может быть зарегистрировано несколько пользователей);

несколько записей о полученном ненормализованном наборе данных о произошедших на узле событиях и инцидентах информационной безопасности (на одном узле может произойти несколько событий и инцидентов);

одна запись о состоянии сетевого узла (один узел может находиться в одном состояний).

Таким образом, все связи будут исполнены по типу «один-ко-многим», за исключением связи «узел» - «состояние», которая будет исполнена по типу «один-к-одному».

Исходя из этого, ER-диаграмма графа Sub_H будет иметь вид, представленный на рисунке 2(б) [5].

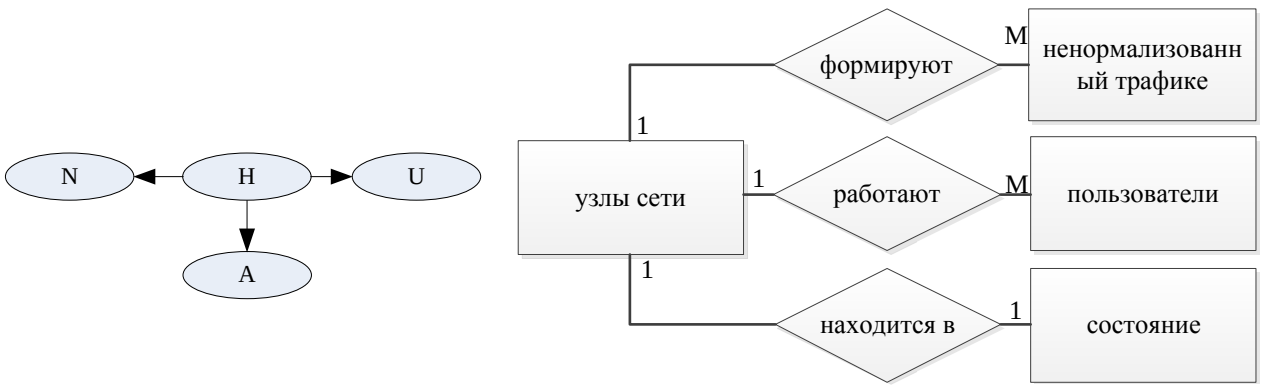


Рис.2 – Взаимосвязь данных о контролируемых узлах сети[2]

[2] Разработано авторами

На рисунке 3(а) представлен подграф Sub_J графа Sup, имеющий следующий вид:

$$Sub_J = \langle D, E/S, H, I, J, M; \{[J, E/S]\} \cup \{[J, I]\} \cup \{[J, D]\} \cup \{[J, H]\} \cup \{[J, M]\} \rangle.$$

Этот граф имеет одно особое отличие от остальных, так как формируется техническими особенностями реализации реляционных баз данных.

Так как на одном узле может быть зарегистрировано несколько событий и инцидентов информационной безопасности, а один инцидент информационной безопасности может затрагивать несколько узлов, то прямая связь между вершинами «узел сети» и «инцидент» («событие») строится по технологии «многие-ко-многим». Тоже самое касается и прямой связи между вершинами «инцидент» («событие») – «урон», «инцидент» («событие») – «рекомендации по ликвидации», «инцидент» («событие») – «цепь событий». Вершина графа «Журнал» позволяет преобразовать все зависимости типа «многие-ко-многим» к типу «один-ко-многим» без потери информативности и оперативности обработки данных.

Таким образом, проявляется связь данных, заносимых в журнал регистрации фактов обнаружения событий и инцидентов информационной безопасности:

с данными о контролируемых узлах;

с данными о произошедших событиях и инцидентах;

с данными о потенциальном или полученном уроне;

с данными, содержащими рекомендации по ликвидации последствий инцидентов информационной безопасности.

При этом одной записи в журнале регистрации будет соответствовать:

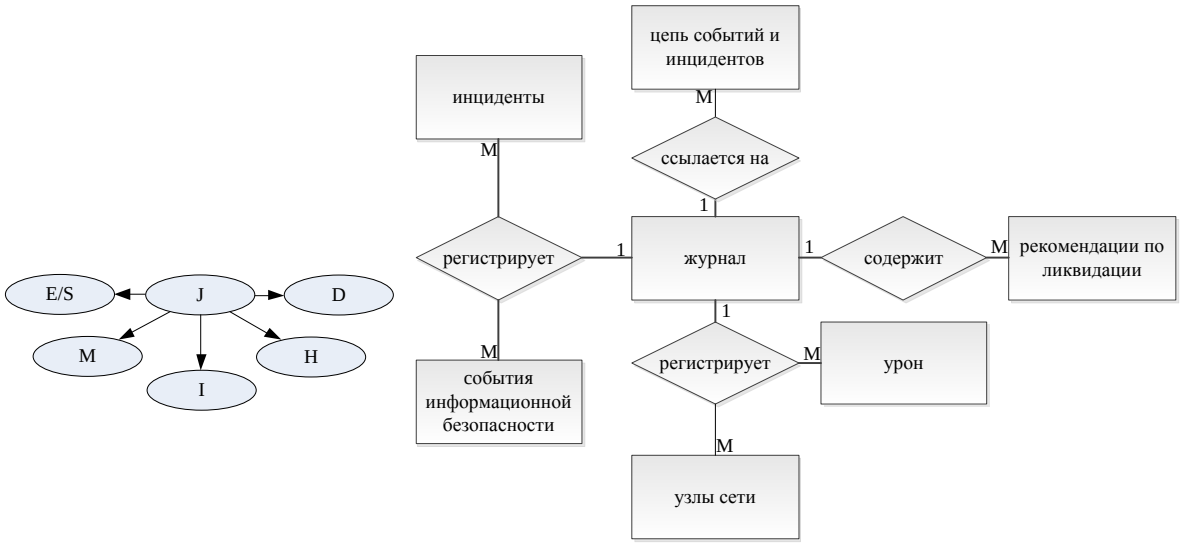
несколько записей о контролируемых узлах (одна запись может описывать состояние нескольких контролируемых узлов);

несколько записей о рекомендациях по ликвидации последствий компьютерного инцидента (одна запись может описывать несколько сценариев ликвидации последствий компьютерного инцидента);

несколько записей о возможной причастности к ранее выявленным цепочкам событий или инцидентов (один и тот же инцидент (событие) может быть звеном в нескольких цепочках событий или атак).

Таким образом, все связи будут исполнены по типу «один-ко-многим».

Исходя из этого, ER-диаграмма графа Sub_J будет иметь вид, представленный на рисунке 3(б).



а) б)

Рис.3 – Взаимосвязь данных о событиях и инцидентах информационной безопасности, занесенных в журнал SIEM-системы[3]

На рисунке 4(а) представлен подграф Sub_M графа Sup, имеющий следующий вид:

$$Sub_M = \langle L, M, P; \{[M, P]\} \cup \{[M, L]\} \rangle.$$

Подграф Sub_M отображает связь данных, содержащих отдельные рекомендации по ликвидации выявленного инцидента, с данными, содержащими отчет по ликвидации инцидента и списка привлекаемого личного состава.

При этом одной записи о рекомендациях по ликвидации инцидента (плана ликвидации) будет соответствовать:

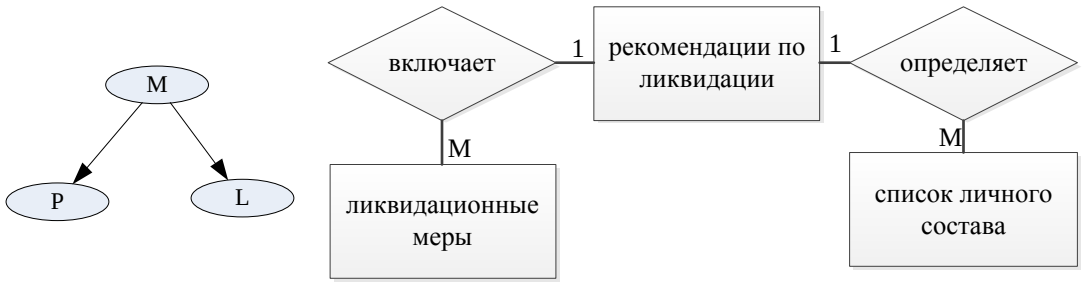
[3] Разработано авторами

несколько записей, содержащих отдельные рекомендации по ликвидации выявленного инцидента (ликвидация одного инцидента может содержать несколько рекомендаций по их устранению);

несколько записей, содержащих данные о привлекаемом личном составе (для ликвидации одного инцидента может быть назначено несколько человек).

Таким образом, все связи будут исполнены по типу «один-ко-многим».

Исходя из этого, ER-диаграмма графа Sub_M будет иметь вид, представленный на рисунке 4(б).



а) б)

Рис.4 – Взаимосвязь данных, описывающих план ликвидации последствий компьютерного инцидента[4]

На рисунке 5(а) представлен подграф Sub_U графа Sup, имеющий следующий вид:

$$Sub_U = \langle K, U; \{[U, K]\}.$$

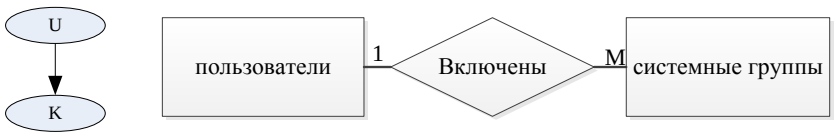
подграф Sub_U отображает связь данных о зарегистрированных в системе пользователях, с данными о системных группах, в которые зачислены эти пользователи.

При этом одной записи о зарегистрированных в системе пользователях будет соответствовать несколько записей о списках системных групп, в которых зарегистрированы пользователи (один пользователь может быть зарегистрирован в нескольких группах)

Таким образом, эта связь будет исполнена по типу «один-ко-многим».

[4] Разработано авторами

Исходя из этого, ER-диаграмма графа Sub_U будет иметь вид, представленный на рисунке 5(б).



а) б)

Рис.5 – Взаимосвязь данных о пользователях, зарегистрированных в контролируемых автоматизированных системах

На рисунке 6(а) представлен подграф $Sub_{A,}$ графа Sup, имеющий следующий вид:

$$Sub_A = \langle A, B, F, G_l / G_g, O, R; \{[A, G_l / G_g]\} \cup \{[A, B]\} \cup \{[A, R]\} \cup \{[A, F]\} \cup \{[A, O]\} \rangle.$$

Подграф $Sub_{A,}$ отображает связь данных о состоянии контролируемых узлов сети с данными об активах, формирующих это состояние, таких как:

список установленного программного обеспечения и его состояние;

список эксплуатируемых средств защиты информации;

состояние политик безопасности (локальных и групповых);

состояние аппаратной части;

состояние конфигурационных файлов.

При этом нескольким записям о состоянии контролируемого узла будет соответствовать:

одна запись о списке установленного программного обеспечения (на нескольких узлах может быть установлено одинаковое программное обеспечение);

одна запись о состоянии аппаратной части (несколько узлов может функционировать на аппаратной платформе одной серии и одного производителя);

одна запись о состоянии элементов политики безопасности (несколько узлов может функционировать на основании одной групповой или однотипной локальной политики безопасности);

одна запись о состоянии файлов конфигурации (несколько узлов может содержать однотипные файлы конфигурации).

Таким образом, эти связи будут исполнены по типу «многие-к-одному».

Исходя из этого, ER-диаграмма графа Sub_A будет иметь вид, представленный на рисунке 6(б).

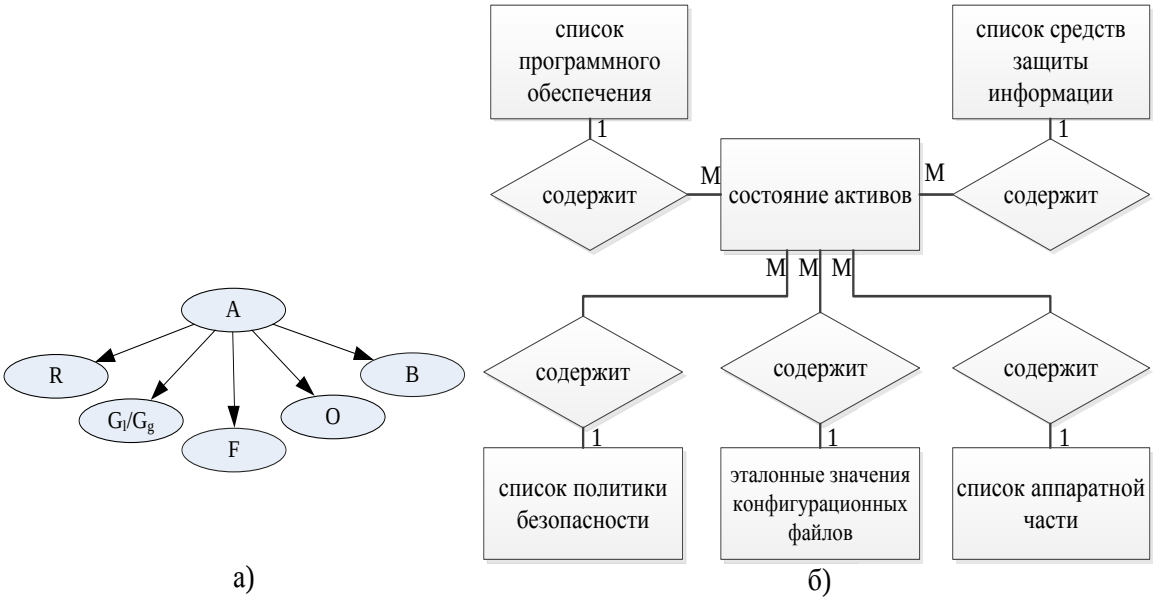


Рис.6 – Взаимосвязь данных о состоянии контролируемых активов[5]

На рисунке 7(а) представлен подграф $Sub_{e/s}$ графа Sup, имеющий следующий вид:

$$Sub_{E/S} = \langle A, E/S, C; \{[E/S, C]\} \cup \{[E/S, A]\} \rangle.$$

Подграф $Sub_{e/s}$ отображает связь данных о выявленных и зарегистрированных событиях и инцидентах информационной безопасности с данными о состоянии контролируемого узла и данными о сетевом взаимодействии.

При этом одной записи о выявленном событии или инциденте информационной безопасности будет соответствовать:

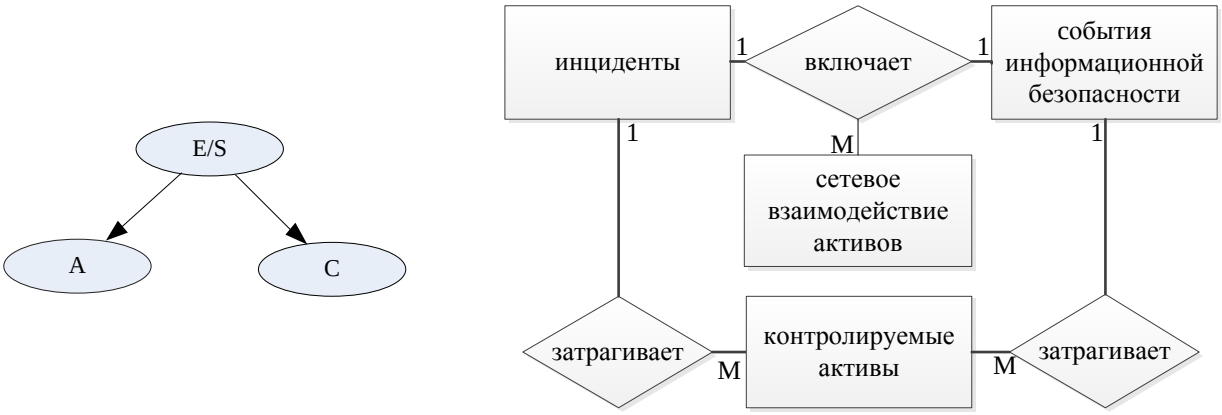
[5] Разработано авторами

несколько записей о сетевом взаимодействии актива (инцидент или событие информационной безопасности может быть выявлен на основании нескольких слепков сетевой активности контролируемого узла);

несколько записей о состоянии контролируемого сетевого узла (инцидент или событие информационной безопасности может затронуть несколько контролируемых узлов, находящихся в разных состояниях).

Таким образом, эта связь будет исполнена по типу «один-ко-многим».

Исходя из этого, ER-диаграмма графа $Sub_{e/s}$ будет иметь вид, представленный на рисунке 7(б).



а) б)

Рис.7 – Взаимосвязь данных о возможных инцидентах информационной безопасности[6]

На рисунке 8(а) представлен подграф Sub_c графа Sup, имеющий следующий вид:

$$Sub_C = \langle C, C'; \{[C, C']\} \rangle.$$

Подграф Sub_c отображает связь данных о сетевом взаимодействии с сохраняемыми слепками трафика сетевого взаимодействия.

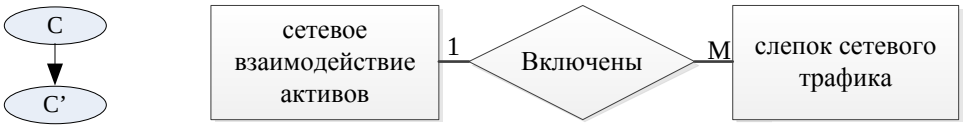
При этом одной записи о сетевом взаимодействии будет соответствовать: несколько записей, характеризующих слепок сетевого взаимодействия (в

[6] Разработано авторами

пределах одной сетевой сессии может быть сформировано несколько слепков сетевого взаимодействия).

Таким образом, эта связь будет исполнена по типу «один-ко-многим».

Исходя из этого, ER-диаграмма графа Sub_c будет иметь вид, представленный на рисунке 8(б).



а) б)

Рис.8 – Взаимосвязь данных о сетевом взаимодействии контролируемых активов[7]

Для получения полной картины взаимосвязи различных данных о событиях и инцидентах информационной безопасности необходимо произвести объединение всех построенных ER-диаграмм. Результирующая ER-диаграмма представлена на рисунке 9.

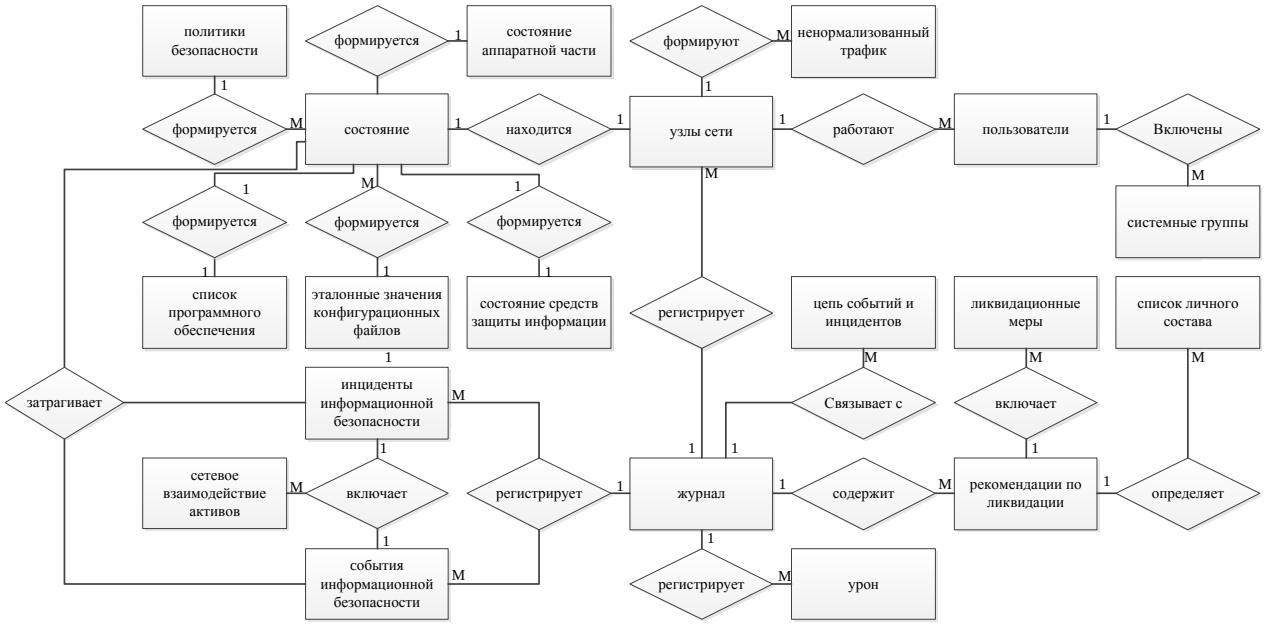


Рис.9 – Полная ER-диаграмма данных о событиях и инцидентах информационной безопасности[8]

[7] Разработано авторами
[8] Разработано авторами

Вывод: Таки образом, проведенная работа по определению характеристик и типов связи между данными о событиях и инцидентах информационной безопасности позволила:

определить детальную структуру данных о событиях и инцидентах информационной безопасности;

сформировать структуру сущностей о событиях и инцидентах информационной безопасности и их взаимосвязей;

определить зависимости данных о событиях и инцидента информационной безопасности;

устранить избыточность данных о событиях и инцидентах информационной безопасности.

Библиографический список

1. **Королев И.Д.** Обзор SIEM - систем: проприетарные ArcpSide и MaxPatrol против OpenSorce решений / И.Д. Королев, Е.С. Литвинов, В.И. Попов, С.А. Коноваленко // Дневник науки. - 2019. – №4. - С. 26-34.

2. **Коноваленко С.А.** Оценка эффективности процессов функционирования подсистемы выявления уязвимостей автоматизированной системы военного назначения / С.А. Коноваленко, И.О. Овчаренко, М.С. Помещиков – Текст: непосредственный // Основные направления развития систем вооружений авиации Воздушно-космических сил. Авиационная техника и вооружение Воздушно-космических сил России и иностранных государств. Безопасность полетов авиации ВКС. Системы ми средства защиты информации: материалы научно-методической конференции / ЦНИИ ВВС Министерства обороны России. – Щелково, 2018. – С. 347–361.

3. **Королев И.Д.** Анализ потоков данных о событиях и инцидентах информационной безопасности, поступающих из разнородных источников / Е.С. Литвинов, И.Д. Королев, С.В. Пестов – Текст: непосредственный //

Материалы международного центра научного сотрудничества "Наука и просвещение", сборник статей VIII всероссийской научно-практической конференции – Пенза: 2020. – С. 26-34.

4. **Судоплатов, С.В.** Дискретная математика: Виды и способы задания графов: учебник: [Издание второе, переработанное] / С.В. Судоплатов, Е.В. Овчинникова; Министерство образования и науки Российской Федерации, Новосибирский государственный университет – М.: ИНФРА-М, 2007. – 255 с. : с. 107–113.

5. **Советов, Б.Я.** Базы данных: теория и практика: создание и использование БД : учебник для бакалавров / Б.Я. Советов, В.В. Цехановский, В.Д. Чертовской – М.: Издательство Юрайт, 2012. – 263 с. : с. 119–150.