ОРГАНИЗАЦИЯ РАЗДЕЛЬНОГО ХРАНЕНИЯ ДАННЫХ О СОБЫТИЯХ БЕЗОПАСНОСТИ

Кузнецов А. В.[1]

DOI: 10.21681/2311-3456-2024-2-22-28

Целью исследования *является повышение эффективности долговременного хранения данных о событиях безопасности за счет организации и применения схемы раздельного хранения данных.*

Метод исследования: *анализ влияния доступной ширины полосы пропускания используемого канала связи на выбор схемы реализации раздельного хранения данных о событиях безопасности; анализ влияния заданных сроков «горячего» и «холодного» хранения данных о событиях безопасности, необходимости хранения исходных и нормализованных данных, а также количества реплик и уровня RAID на физический (фактический) объем подсистемы хранения данных о событиях безопасности.*

Результаты исследования: *1) Определены условия для выбора схем реализации подсистем «горячего» и «холодного» хранения данных о событиях безопасности, которые в отличие от известных учитывают доступную ширину полосы пропускания используемого канала связи между коллектором для сбора событий SIEM-системы и компонентами «горячего» хранения, а также между компонентами «горячего» и «холодного» хранения, что позволяет сократить расходы и разделить использование SSD и HDD носителей данных. 2) Разработана методика расчета физического объема подсистемы хранения SIEM-системы, которая в отличие от известных учитывает наличие заданных сроков «горячего» и «холодного» хранения данных о событиях безопасности, необходимость хранения исходных и нормализованных данных, а также количество реплик и уровень RAID, что позволяет оперировать не эффективным, а реальным объемом носителей данных.*

Применение результатов настоящего исследования дает положительный эффект в области технических наук и позволяет внести значительный вклад в развитие центров мониторинга ИБ (SOC), включая центры ГосСОПКА, и операторов ГИС федерального или регионального масштабов, а также формирует основу для применения Data Driven Decision Making подхода и машинного обучения в рамках обеспечения ИБ современных организаций.

Ключевые слова: *подсистема хранения данных, «горячее» хранение, «холодное» хранение, инцидент информационной безопасности, ГосСОПКА, security information and event management, events per second, redundant array of independent disks.*

THE ORGANIZATION OF SEPARATE SECURITY EVENT DATA STORAGE

Kuznetsov A. V.[2]

Purpose of work *is to improve the efficiency of long-term storage of security event data by organizing and implementing of the separate data storage scheme.*

Research method: *analysis of the influence of available communication channel bandwidth on separate security event data storage scheme choosing; analysis of the influence of specified terms of «hot» and «cold» storage of security event data, the need to store raw and normalized data, as well as replica number and RAID level on the physical (real) volume of an event data storage subsystem.*

Result of the study: *a) The conditions for «hot» and «cold» security event data storages scheme choosing are developed, which unlike the known ones take into account the available communication channel bandwidth between the collector of SIEM system events and «hot» storage components, as well as between «hot» storage components and «cold» storage components, which allows to reduce costs and to separate using*

1 Кузнецов Александр Васильевич, кандидат технических наук, CISM, CISSP, руководитель группы архитектуры ООО «РТК ИБ», Москва, Россия. ORCID: 0000-0002-7160-1845. E-mail: 1283_my@mail.ru

2 Aleksandr V. Kuznetsov, Ph.D. (in Tech.), CISM, CISSP, architecture team leader RTK IS LLC, Moscow, Russia. ORCID: 0000-0002-7160-1845. E-mail: 1283_my@mail.ru

of SSD and HDD data drivers b) The methodology for calculating the physical volume of a SIEM system storage subsystem is developed, which unlike the known ones takes into account specified terms of «hot» and «cold» storage of security event data, the need to store raw and normalized data, as well as replica number and RAID level, which allows to operate with real volume of data drivers rather than effective volume.

The application of this study results has a positive effect in the field of technical sciences and allows to make a significant contribution to the development of Security Operations Center (SOC), including GosSOPKA centers, and GIS operators of federal or regional scale. It also forms the basis for the application of Data Driven Decision Making approach and machine learning within establishing and maintenance information security of modern organizations.

Keywords: *data storage subsystem, hot storage, cold storage, information security incident, GosSOPKA, security information and event management, events per second, redundant array of independent disks*

Введение

Регистрируемая информация о событиях безопасности (записи о событиях безопасности)[3] является неотъемлемой частью входных данных, используемых в рамках реализации процессов обнаружения и приоритизации инцидентов информационной безопасности (ИБ) в совокупности с сетевым трафиком (дампами сетевого трафика) и телеметрическими данными [1]. А в рамках ретроспективного анализа собранных данных (threat hunting) [2, 3] и расследований инцидентов ИБ (forensic) [4, 5] данные о событиях безопасности зачастую выступают единственным источником информации о действиях нарушителя, т.е. их надлежащее хранение является важной задачей.

При этом стоит отметить, что для крупных информационно-телекоммуникационных (ИТ) инфраструктур потоки данных о событиях безопасности могут достигать десятков и сотен тысяч единиц в секунду (events per second (EPS)), а в ряде случаев даже миллионов EPS. При среднем размере одной записи о событии безопасности в 600 Байт, общий объем сохраняемых данных начнет превышать 1 Тбайт в день, начиная с потока всего в 21 222 EPS. При этом стоит отметить, что определение среднего размера одной записи о событии безопасности, релевантной для соответствующей ИТ-инфраструктуры, является отдельной исследовательской задачей, которая находится за рамками настоящего исследования.

К сожалению, на сегодняшний день действующими нормативно-методическими документами и стандартами не предусмотрены единые сроки хранения собранных данных о событиях безопасности:

- ✓ хранение данных в течение как минимум трех лет[4];
- ✓ хранение данных в течение не менее одного года, причем в оперативном доступе должны находиться данных не менее чем за последние три месяца[5];
- ✓ хранение данных не менее трех месяцев[6];
- ✓ хранение агрегированных данных о событиях безопасности не менее шести месяцев[7].

На практике в качестве нижней границы сроков хранения данных о событиях безопасности зачастую выступают три месяца, а верхняя граница регулируется внутренними нормативными документами конкретной организации (месяцы – годы), т.е. в любом случае речь будет идти о десятках и сотнях терабайт сохраняемых данных, а для очень крупных ИТ-инфраструктур – о петабайтах данных, соответственно, для хранения потребуются значительные вычислительные ресурсы, в первую очередь, носители данных.

Здесь необходимо отметить, что в связи с тем, что требования к скорости операций чтения и записи данных снижаются в течение выбранного срока хранения, для крупных ИТ-инфраструктур экономически нецелесообразно организовывать хранение данных о событиях безопасности в течение всего срока хранения на одном типе носителей, а именно на Solid State Drive (SSD), т.к. у Hard (Magnetic) Disk Drive (HDD) более низкая цена за терабайт [6, 7], т.е. целесообразно рассмотреть, как минимум, два раздельных режима хранения данных: «горячее» (hot) на SSD и «холодное» (cold) хранение на HDD носителях данных. Архивное хранение находится за рамками настоящего исследования, т.к. к архивным данным нет прямого доступа и поиск по ним не возможен без проведения предварительных мероприятий, в том числе по выделению места на активной подсистеме хранения для разархивирования этих данных.

3 ГОСТ Р 59548-2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации».

4 Стандарт Банка России СТО БР ИББС-1.3-2016 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств».

5 Payment Card Industry Data Security Standard.

6 Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах» от 11.02.2014 г.

7 «Требования к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты», утв. приказом ФСБ России от 06.05.2019 N 196.

Таким образом, повышение эффективности долговременного хранения данных о событиях безопасности за счет организации и применения схемы раздельного хранения данных является актуальной задачей, в том числе крайне востребованной в крупных организациях федерального или регионального масштаба, в первую очередь, являющихся операторами государственных информационных систем (ГИС) и/или субъектами Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА).

Схемы организации раздельного хранения данных о событиях безопасности

В рамках настоящего исследования организация раздельного хранения данных о событиях безопасности будет рассматриваться для средств управления событиями безопасности (Security Information and Event Management, далее – SIEM-систем), поддерживающих высоконагруженные инсталляции в десятки и сотни тысяч EPS и сертифицированных по требованиям безопасности информации[8], например:

- ✓ Kaspersky Unified Monitoring and Analysis Platform;
- ✓ MaxPatrol SIEM;
- ✓ KOMRAD Enterprise SIEM.

Подсистема хранения SIEM-системы может быть реализована в формате нескольких схем, представленных в таблице (табл.1):

- ✓ централизованное хранение (например, в едином центре обработки данных (ЦОД));
- ✓ децентрализованное хранение на ряде выделенных площадок (например, в нескольких региональных ЦОД);
- ✓ локальное хранение на каждой площадке, где осуществляется сбор данных о событиях безопасности (например, в каждом филиале организации, территориальном органе или т.п.)

Таблица 1

Взаимосвязь схем реализации подсистем «горячего» и «холодного» хранения данных о событиях безопасности

№ п/п	«Холодное» хранение / «Горячее» хранение	Централизованное	Децентрализованное	Локальное
1	Централизованное	+	–	–
2	Децентрализованное	+	+	–
3	Локальное	+	+	+

8 Государственный реестр сертифицированных средств защиты информации: https://reestr.fstec.ru/reg3

Примеры наиболее популярных схем раздельного хранения данных представлены на рисунках (рис.1, рис.2, рис.3).

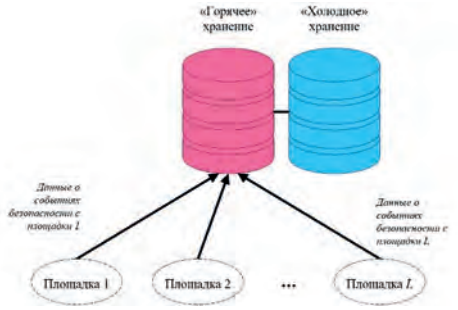

Рис. 1. Централизованное «горячее» и «холодное» хранение данных

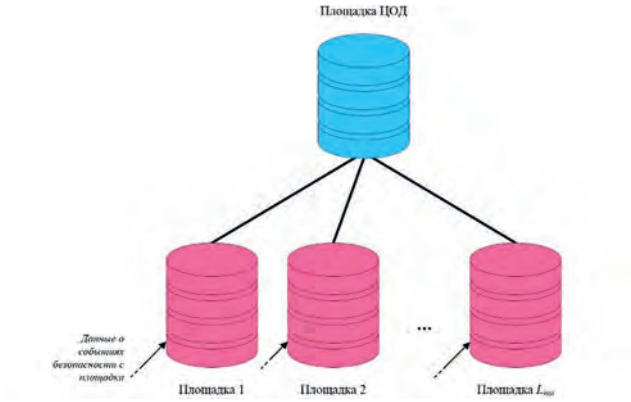

Рис. 2. Локальное «горячее» и централизованное «холодное» хранение данных

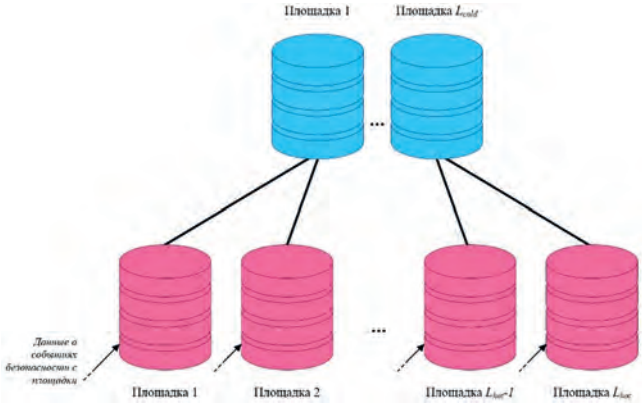

Рис. 3. Локальное «горячее» и децентрализованное «холодное» хранение данных

Ключевыми преимуществами централизации подсистемы хранения данных о событиях безопасности являются сокращение затрат на управление и обслуживание подсистемы хранения данных, а также упрощение обработки данных, включая поиск (анализ) по единому хранилищу. Ключевыми преимуществами децентрализации и локализации подсистемы хранения данных о событиях безопасности являются повышение катастрофоустойчивости

подсистемы хранения данных, а также снижение нагрузки на каналы передачи данных. Данные преимущества и «зеркальные» им недостатки будут выступать ориентирами при выборе конкретной схемы для отдельно взятой организации.

При этом в качестве ключевого параметра, влияющего на выбор схемы реализации подсистемы хранения данных о событиях безопасности, в рамках настоящего исследования будет рассматриваться только доступная ширина полосы пропускания используемого канала связи между коллектором(ами) для сбора событий SIEM-системы и компонентами «горячего» хранения, а также между компонентами «горячего» и «холодного» хранения. Данный параметр выбран по причине того, что он является первичным техническим стоп-фактором и не может быть компенсирован другими параметрами или мероприятиями.

Предлагается следующее условие, определяющее возможность централизации подсистемы хранения данных на одной выделенной площадке:

$$(S + 58) \cdot E \cdot 8 \cdot 9{,}54 \cdot 10^{-7} \le B, \quad (1)$$

где $S \in [0;+\infty)$ – размер одной передаваемой записи о событии безопасности, Байт; $E \in [0;+\infty)$ – усредненный за сутки поток данных о событиях безопасности, ед./с; $B \in [0;+\infty)$ – доступная ширина полосы пропускания используемого канала связи, Мбит/с; 58 Байт – это служебные данные в формате максимального суммарного размера заголовка для Ethernet-фрейма, IP-пакета и TCP-сегмента или UDP-датаграммы, а также контрольной суммы Ethernet-фрейма.

Если условие (1) не выполняется, то дальше рассматривается схема децентрализованного хранения данных о событиях безопасности, где аналогичное условие применятся к каждой из выделенных площадок:

$$(S + 58) \cdot E \cdot 8 \cdot 9{,}54 \cdot 10^{-7} \le B_i, \quad (2)$$

где $i \in [1;L]$ и L – количество выделенных площадок.

Если условия (2) для выделенных площадок не выполняются, то дальше рассматривается только схема локального хранения данных о событиях безопасности на каждой площадке, где осуществляется их сбор.

Принимая во внимание, что поток данных о событиях безопасности не является фиксированным [8, 9], в том числе из-за того, что реализация угроз безопасности информации носит случайный характер [10, 11], а также широковещательный трафик в сети составляет примерно 20% [12], целесообразно утилизировать доступную ширину полосы пропускания в диапазоне 60–80% (табл.2).

Значения более 100% означают недостаточность предлагаемого канала связи для функционирования SIEM-системы (данные о событиях безопасности будут поступать с задержками или не будут доставлены в подсистему хранения данных). Значения менее 60% означают неэффективное использование предлагаемого канала связи (данный канал и сетевой интерфейс подсистемы хранения данных можно совмещать для решения других задача).

Методика расчета необходимого дискового пространства

Постановка задачи: расчет физического (фактического) объема подсистемы хранения SIEM-системы в условиях наличия заданных сроков «горячего» и «холодного» хранения данных о событиях безопасности, а также параметров отказоустойчивости подсистемы хранения данных.

В качестве параметров отказоустойчивости подсистемы хранения данных в рамках настоящего исследования будут рассматриваться:

- ✓ на уровне данных: количество реплик (копий данных);
- ✓ на аппаратном уровне: избыточность массива независимых дисков (Redundant Array of Independent Disks (RAID)).

Существующие работы по организации подсистем хранения данных о событиях безопасности акцентируют свое внимание на отказоустойчивости

Таблица 2

Результаты вычисления утилизации потоком данных о событиях безопасности доступной ширины полосы пропускания используемого канала связи (S=600 Байт)

№ п/п	Шир. полосы пропускания		Поток данных о событиях безопасности к подсистеме хранения, ед./сек								
			10 000	25 000	50 000	75 000	100 000	150 000	200 000	250 000	500 000
1	Требуемая шир. полосы пропускания, Мбит/с		50,22	125,55	251,09	376,64	502,19	753,28	1 004,37	1 255,46	2 510,93
2	% от доступной шир. полосы пропускания в Мбит/с	100	50,22	125,55	251,1	376,64	502,19	753,28	1 004,38	1 255,47	2 510,93
3		256	19,62	49,05	98,09	147,13	196,17	294,25	392,34	490,42	980,84
4		512	9,81	24,53	49,05	73,57	98,09	147,13	196,17	245,21	490,42
5		768	6,54	16,35	32,7	49,05	65,39	98,09	130,78	163,48	326,95
6		1 024	4,91	12,27	24,53	36,79	49,05	73,57	98,09	122,61	245,21
7		1 536	3,27	8,18	16,35	24,53	32,7	49,05	65,39	81,74	163,48
8		2 048	2,46	6,14	12,27	18,4	24,53	36,79	49,05	61,31	122,61

на аппаратном уровне [13, 14] или на повышении эффективности хранения за счет применения нереляционных (NoSQL) баз данных [15, 16] и не уделяют достаточное внимание особенности хранения данных о событиях безопасности в SIEM-системах, а именно: хранению и исходных (raw), и нормализованных данных. А материалы производителей SIEM-систем оперируют приблизительными (экспертными) расчетами требуемого эффективного объема[9] или оставляют решение данной целиком задачи проектной команде. Таким образом, существующие работы и материалы не в полной мере позволяют решить поставленную актуальную задачу.

Предлагаемая методика расчета необходимого дискового пространства включает в себя следующие шаги и применяется последовательно, начиная с «горячего» хранения:

- ✓ 1 шаг: определение схемы реализации подсистем хранения данных о событиях безопасности согласно предыдущему разделу и определение количества хранилищ (площадок для хранения): L_{hot} и L_{cold}.
- ✓ 2 шаг: определение срока хранения данных для каждого типа хранилища и площадок (в случае необходимости) в днях: $D_{hot\,i}$ и $D_{cold\,j}$, где $i \in [1;L_{hot}]$ и $j \in [1;L_{cold}]$.
- ✓ 3 шаг: установление количества реплик: R_1, шт.;
- ✓ 4 шаг: вычисление эффективного дискового объема подсистемы хранения SIEM-системы V_i в терабайтах по формуле:

$$V_i = \left(\left(\frac{E_i \cdot 86\,400 \cdot D_{hot\,i} \cdot (S + N) \cdot K}{1\,099\,511\,627\,776}\right) + F_i \cdot D_{hot\,i}\right) \cdot R_1, \quad (3)$$

где $E_i \in [0;+\infty)$ – усредненный поток данных о событиях безопасности на i-ой площадке за сутки, ед./с; $S \in [0;+\infty)$ – размер одной исходной записи о событии безопасности, Байт; $N \in [0;S]$ – размер одной нормализованной записи о событии безопасности, Байт; $K \in (0;1]$ – коэффициент сжатия, который напрямую зависит от возможностей используемой системы управления базами данных в составе подсистемы хранения SIEM-системы, определение его значения находится за рамками настоящего исследования, по умолчанию рассматриваться худший сценарий, когда $K = 1$; $F_i \in [0;+\infty)$ – размер данных NetFlow или т.п. на i-ой площадке за сутки, ТБ/день; $R_1 \in [2;+\infty)$ – количество реплик (копий данных), ед.

Формула (3) не учитывает метаданные (служебные данные). Если они возникают в рамках функционирования конкретной системы управления базами данных, то их объем необходимо учесть в V_i.

9 Эксплуатационный документ «Руководство по внедрению MaxPatrol SIEM версия 7.2»

- ✓ 5 шаг: определение поправочного коэффициента за счет применения требуемого уровня RAID – R_2, согласно таблице (табл.3) [13, 17], где $n \in [0;+\infty)$ – количество накопителей данных одного размера. Оценка показателей безотказности, в том числе построение функции надежности, находится за рамками настоящего исследования.

Таблица 3

Сведения о популярных уровнях избыточности массива независимых дисков (RAID)

№ п/п	Уровень RAID	Минимальное количество накопителей, шт.	Значение поправочного коэффициента
1	RAID 0	2	1
2	RAID 1	2	0,5
3	RAID 5	3	$1 - 1/n$
4	RAID 6	4	$1 - 2/n$
5	RAID 10 (RAID 1+0)	4, четное число накопителей	0,5
6	RAID 50 (RAID 5+0)	6, четное число накопителей	$1 - 2/n$
7	RAID 60 (RAID 6+0)	8, четное число накопителей	$1 - 4/n$

- ✓ 6 шаг: вычисление физического (фактического) дискового объема подсистемы хранения SIEM-системы W_i в терабайтах по формуле:

$$W_i = \frac{V_i}{R_2} \quad (4)$$

- ✓ 7 шаг: выполнение шагов 1–6 для подсистемы «холодного» хранения с учетом:
  - требуемого количества хранилищ (площадок для хранения): L_{cold}, ед.;
  - требуемого срока «холодного» хранения данных для каждого хранилища (площадок для хранения): $D_{cold\,j}$, дни;
  - требуемого уровня RAID – R_2, для подсистемы «холодного» хранения согласно таблице (табл. 3).

По результатам применения предложенной методики будут получены два значения:

- ✓ W_i для каждого «горячего» хранилища (площадок для «горячего» хранения), где $i \in [1;L_{hot}]$;
- ✓ W_j для каждого «холодного» хранилища (площадок для «холодного» хранения), где $j \in [1;L_{cold}]$.

Примеры расчетных значений

Варианты расчетных значений для разных потоков данных о событиях безопасности, разных длительностей хранения и уровней RAID, но фиксированном $R_1 = 2$ реплики, $S = 600$ Байт, $N = 300$ Байт, $K = 2/3$, $F_i = 0$, $n = 8$ шт., приведены в таблице (табл. 4).

Таблица 4

Результаты вычисления физического объема подсистемы хранения SIEM-системы

№ п/п	Поток данных к подсистеме хранения, ед./сек	Физический объем подсистемы хранения, ТБ								
		90 дней хранения			180 дней хранения			365 дней хранения		
		RAID 0	RAID 10	RAID 50	RAID 0	RAID 10	RAID 50	RAID 0	RAID 10	RAID 50
1	10 000	85	170	113	170	339	226	344	688	459
2	25 000	212	424	283	424	849	566	860	1 721	1 147
3	50 000	424	849	566	849	1 697	1 132	1 721	3 442	2 295
4	75 000	637	1 273	849	1 273	2 546	1 697	2 581	5 163	3 442
5	100 000	849	1 697	1 132	1 697	3 395	2 263	3 442	6 884	4 589
6	150 000	1 273	2 546	1 697	2 546	5 092	3 395	5 163	10 325	6 884
7	200 000	1 697	3 395	2 263	3 395	6 789	4 526	6 884	13 767	9 178
8	250 000	2 122	4 243	2 829	4 243	8 487	5 658	8 605	17 209	11 473
9	500 000	4 243	8 487	5 658	8 487	16 973	11 316	17 209	34 418	22 945
10	1 000 000	8 487	16 973	11 316	16 973	33 947	22 631	34 418	68 836	45 891

Значения для RAID 0 отражают ситуацию, когда физический объем равен эффективному объему, т.е. минимальный объем подсистемы хранения данных в условиях наличия заданных сроков хранения (нижняя граница). Значения для RAID 10 отражают ситуацию, когда физический объем равен удвоенному эффективному объему, т.е. максимальный объем подсистемы хранения данных в условиях наличия заданных сроков хранения (верхняя граница).

Заключение

По результатам проведенного исследования:

1. Определены условия для выбора схем реализации подсистем «горячего» и «холодного» хранения данных о событиях безопасности, которые в отличие от известных учитывают доступную ширину полосы пропускания используемого канала связи между коллектором(ами) для сбора событий SIEM-системы и компонентами «горячего» хранения, а также между компонентами «горячего» и «холодного» хранения, что позволяет сократить расходы и разделить использование SSD и HDD носителей данных, т.е. повысить эффективность долговременного хранения данных о событиях безопасности.
2. Разработана методика расчета физического объема подсистемы хранения SIEM-системы, которая в отличие от известных учитывает наличие заданных сроков «горячего» и «холодного» хранения данных о событиях безопасности, необходимость хранения исходных и нормализованных данных, а также количество реплик и уровень RAID, что позволяет оперировать не эффективным, а реальным объемом носителей данных, который необходим для их последующего выбора (заказа), приобретения и эксплуатации.

Применение результатов настоящего исследования дает положительный эффект в области технических наук (методы и системы защиты информации, информационная безопасность). Дополнительно стоит отметит, что увеличение сроков «холодного» хранения за счет оптимизации стоимости подсистемы хранения данных позволит обеспечить и другие процессы управления и обеспечения ИБ необходимыми входными данными [18], что в свою очередь является обязательным условиям для перехода к Data Driven Decision Making подходу и машинному обучению (machine learning) в рамках обеспечения ИБ современных организаций [19, 20].

Внедрение раздельного (дифференцированного) хранения данных о событиях безопасности позволит внести значительный вклад в развитие центров мониторинга ИБ (Security Operations Center (SOC)), в том числе центров ГосСОПКА, и операторов ГИС федерального или регионального масштаба.

Предложенная методика была апробирована в рамках выполнения проектных работ в 2023 г. силами ООО «РТК ИБ» для ИТ-инфраструктуры организации, являющейся оператором ГИС федерального масштаба, субъектом критической информационной инфраструктуры, субъектом ГосСОПКА, с суммарным потоком данных о событиях безопасности более 200 000 EPS.

DOI: 10.21681/2311-3456-2024-2-22-28

Литература

1. *A. Barros, A. Chuvakin, A. Belak. Applying Network-Centric Approaches for Threat Detection and Response // Gartner, Inc. | G00373460. 2019. pp. 1–37.*
2. *Котенко И. В., Попков И. А. Методика автоматизированного сбора криминалистических данных в процессах threat hunting // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). Сборник научных статей. XII Международная научно-техническая и научно-методическая конференция. В 4 т. Санкт-Петербург, 2023. С. 679–683.*
3. *Yang F., Han Ya., Ding Y., Tan Q., Xu Zh. A Flexible Approach for Cyber Threat Hunting Based on Kernel Audit Records // Cybersecurity. 2022. Т. 5. № 1. С. 1–16.*
4. *Федотов Н. Н. Форензика – компьютерная криминалистика // М.: Юридический Мир, 2007. С. 139–144.*
5. *M. Yahia. Effective Threat Investigation for SOC Analysts // Packt Publishing Ltd. pp. 15-17, 49-204. ISBN 978-1-83763-478-1.*
6. *Пономарев В. А. Моделирование и оптимизация функционирования твердотельной системы хранения данных: дис. ... канд. техн. наук. Москва. 2019. С. 5, 53–81.*
7. *Шарапов Р. В. Аппаратные средства хранения больших объемов данных // Инженерный вестник Дона. 2012. № 4–2 (23). С. 67.*
8. *Шеремет И. А., Кузнецов А. В. Идентификация угроз информационной безопасности специализированных автоматизированных систем финансовых организаций с применением комбинированной обработки потоков информации о событиях безопасности // В сборнике: Информационная безопасность в банковско-финансовой сфере. Сборник научных работ участников ежегодной международной молодежной научно-практической конференции в рамках V Международного форума «Как попасть в пятерку?». 2018. С. 175–178.*
9. *Королев И. Д., Литвинов Е. С., Пестов С. В. Анализ потоков данных о событиях и инцидентах информационной безопасности, поступающих из разнородных источников // В сборнике: Результаты современных научных исследований и разработок. сборник статей VIII Всероссийской научно-практической конференции. 2020. С. 26–34.*
10. *Воронин Е. А., Козлов С. В., Кубанков А. Н. Выявление угроз на основе ограниченного набора данных при оценке систем обеспечения безопасности и мероприятий по их реализации // Наукоемкие технологии в космических исследованиях Земли. 2022. Т. 14. № 3. С. 41–48.*
11. *Космачева И. М., Давидюк Н. В., Сибикина И. В., Кучин И. Ю. Модель оценки эффективности конфигурации системы защиты информации на базе генетических алгоритмов // Моделирование, оптимизация и информационные технологии. 2020. Т. 8. № 3 (30). С. 1–14.*
12. *Бражук А. Защита внутри периметра [Электронный ресурс] // Хакер. 2013. Режим доступа: https://xakep.ru/2013/08/23/safe-among-perimetr/.*
13. *Парошин Н. А., Мещеров М. Ш. Анализ надежности и безопасности хранения данных в RAID-системах // Современные научные исследования и инновации. 2023. № 9 (149).*
14. *Борзенкова С. Ю., Савин И. В. Обеспечение безопасности систем хранения данных // Известия Тульского государственного университета. Технические науки. 2017. № 10. С. 196–200.*
15. *Котенко И. В., Саенко И. Б., Полубелова О. В. Перспективные системы хранения данных для мониторинга и управления безопасностью информации // Труды СПИИРАН. 2013. № 2 (25). С. 113–134.*
16. *Котиков П. Е., Тихомирова А. А. Некоторые новые аспекты обеспечения безопасности медицинских данных в системах их хранения // Педиатр. 2017. Т. 8. № S1. С. М165.*
17. *Антипова Т. С. Основные стандарты RAID-массивов // В сборнике: Достижения и приложения современной информатики, математики и физики. материалы VII Всероссийской научно-практической заочной конференции. 2018. С. 511–520.*
18. *Кузнецов А. В. Взаимосвязь процесса управления событиями с другими процессами управления предприятия // Вопросы кибербезопасности. 2017. № 5 (24). С. 17–22. DOI: 10.21681/2311-3456-2017-5-17-22*
19. *Yang N., Yang C., Huang Y., Zhang L., Zhu B., Xing C., Ye D., Jia J., Chen D., Shen X. Deep Learning-based SCUC Decision-making: An Intelligent Data-driven Approach with Self-learning Capabilities // IET Generation, Transmission & Distribution. 2021. DOI: 10.1049/gtd2.12315*
20. *Sarker I. H., Kayes A. S. M., Watters P., Ng A., Badsha S., Alqahtani H. Cybersecurity Data Science: An Overview from Machine Learning Perspective // Journal of Big Data. 2020. Т. 7. № 1. pp. 1 41. DOI: 10.1186/s40537-020-00318-5*