КОМПЛЕКСНЫЕ РЕШЕНИЯ ДЛЯ МИНИМИЗАЦИИ ВНУТРЕННИХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Морозов В. Е.[1], Милославская Н. Г.[2]

DOI: 10.21681/2311-3456-2024-5-67-78

Цель работы: *определение состава современных решений, в совокупности позволяющих создать систему комплексного управления информационной безопасностью организации.*

Методы исследования: *анализ релевантных научных публикаций, концептуальное моделирование, экспертная оценка, синтез системы комплексного управления информационной безопасностью.*

Полученные результаты: *в статье детализируются составляющие процесса управления информационной безопасностью (ИБ) и обсуждается возможный состав ориентированной на минимизацию внутренних угроз системы комплексного управления ИБ организации. Показано, что подобная система должна включать следующие ключевые элементы: подсистему централизованного мониторинга событий и расследования инцидентов ИБ, подсистему контроля защищенности данных и выявления уязвимостей в доступе к ним, а также подсистему контроля информационных потоков и противодействия утечкам защищаемой информации. Указанные подсистемы могут быть реализованы при помощи SIEM-, DCAP- и DLP-систем соответственно. Рассматриваются основные концепции и технологии, на базе которых разработаны данные решения, их архитектура, особенности функционирования и аналитические возможности на примере программных комплексов, разработанных компанией «СёрчИнформ» («СёрчИнформ SIEM», «СёрчИнформ FileAuditor» и «КИБ СёрчИнформ»). Анализ совокупности характеристик и опыта применения названных продуктов показывает, что при условии их интеграции они способны обеспечить полномасштабную защиту деятельности организации на всех уровнях.*

Практическая значимость *заключается в обосновании достаточности указанного состава системы управления ИБ для решения задачи минимизации внутренних угроз.*

Ключевые слова: *DLP, DCAP, SIEM, внутренние угрозы информационной безопасности, инцидент информационной безопасности, мониторинг, событие информационной безопасности, управление информационной безопасностью.*

Введение

Эксперты во всем мире ежегодно фиксируют значительный рост числа инцидентов информационной безопасности (ИБ)[3], среди которых фигурируют регулярно обнаруживаемые в открытом доступе «утёкшие» персональные данные, «сливы» внутренних документов различных компаний[4], случаи заражения вредоносным кодом с последующим уничтожением данных и многое другое. Сам по себе данный факт уже давно не вызывает ни у кого удивления – это сформировавшаяся устойчивая тенденция, наблюдающаяся в течении ряда последних лет. Однако, начиная с 2022 г., в Российской Федерации рост числа инцидентов ИБ приобрел по-настоящему взрывной характер. Помимо рядовых граждан от киберпреступлений часто страдает и критическая информационная инфраструктура (КИИ), которой граждане, к слову, активно пользуются – транспортной, финансовой, медицинской, энергетической, промышленной [1,2]. Одной из основных причин большого числа уязвимостей в программном обеспечении (ПО) объектов КИИ является уход иностранных вендоров, которые перестали поддерживать свои решения, ранее установленные у российских заказчиков. В то же время отечественные аналоги еще только начинают свое движение навстречу российским клиентам [3]. А если прибавить к увеличившейся интенсивности атак дефицит квалифицированных ИБ-специалистов, то становится очевидно, что в службах ИБ и государственных корпораций, и коммерческих компаний не последнюю роль должны играть комплексные решения, позволяющие защитить данные сразу по нескольким направлениям в сочетании с эффективным управлением ИБ.

Источники угроз ИБ многообразны и могут находиться как снаружи защищаемого периметра организации, так и внутри него. Принято считать, что именно внутренние угрозы представляют наибольшую опасность, так как именно на них приходится большинство фиксируемых инцидентов ИБ. Случайные ошибки персонала, бездействие, мошенничество,

1 Морозов Виктор Егорович, кандидат психологическин наук, доцент. ООО «Либрасофт», Минск, Республика Беларусь. E-mail: v.morozov@searchinform.ru
2 Милославская Наталья Георгиевна, доктор технических наук, Ph.D. in Cybersecurity, доцент. НИЯУ МИФИ, Москва, Россия. E-mail: NGMiloslavskaya@mephi.ru

3 Тренды кибератак на промышленность и телеком [Электронный ресурс] // Solar. URL: https://rt-solar.ru/analytics/reports/4361/ (дата обращения: 05.08.24).
4 Рахметов, Р. Что такое DLP системы и как они применяются [Электронный ресурс] // Security Vision. URL: https://www.securityvision.ru/blog/chto-takoe-dlp-sistemy-i-kak-oni-primenyayutsya/ (дата обращения: 05.08.24).

Рис. 1. Составляющие процесса управления ИБ

инсайдерские действия регулярно приводят к многомиллионному ущербу для компаний, работающих в сфере высоких технологий, финансов, связи.

Управление ИБ в общем случае представляет собой циклический процесс, который включает в себя сбор и анализ данных об уровне ИБ в организации, оценку рисков ИБ, планирование мер по их обработке, реализацию и внедрение соответствующих мер обеспечения ИБ (ОИБ) [4], распределение ролей и ответственности, оперативную работу по осуществлению мероприятий по защите, мониторинг функционирования мер ОИБ, оценку их эффективности и соответствующую коррекцию в зависимости от результатов деятельности (рис. 1). В техническом плане управление ИБ можно разделить на использование локальных подсистем мониторинга и управления отдельными средствами защиты информации и создание комплексных систем управления ИБ[5] [5–8].

В настоящее время на рынке программных продуктов, ориентированных на ОИБ, представлено достаточно большое число классов различных решений[6], среди которых следует выделить следующие: *SOAR* (*Security Orchestration, Automation and Response*), *SIEM* (*Security Information and Event Management*), *DLP* (*Data Loss Prevention*), *XDR* (*Extended Detection and Response*), *EDR* (*Endpoint Detection and Response*), *DFIR* (*Digital Forensics and Incident Response*). В последние годы к ним добавились еще и системы, разработанные в рамках подхода *DCAP/DAG* (*Data-Centric Audit and Protection/Data Access Governance*)[7]. Тем не менее, сложно представить себе ситуацию, чтобы в одной организации использовались сразу все перечисленные системы. Да и практика чаще всего подталкивает к разумным ограничениям: далеко не каждая компания готова выделить достаточные финансовые и технические ресурсы для приобретения и эксплуатации всего вышеперечисленного. Поэтому нередко встают вопросы об оптимальном наборе ИБ-решений, о перечне ключевых систем, о проектировании и организации целевой архитектуры ИБ, учитывающей специфику конкретной организации или проекта, и т.п.

Все сказанное выше вольно или невольно подталкивает к определению своего рода базового набора средств, актуальных сегодня для любой организации и позволяющих достичь комплексности ОИБ. При этом не стоит забывать, что на практике крайне важно оценить конкретные потребности и цели организации, прежде чем выбирать средства, которые лучше всего будут удовлетворять этим потребностям.

Для начала попробуем выделить ключевые элементы системы комплексного управления ИБ. К ним следует отнести:

- подсистему централизованного мониторинга событий и расследования инцидентов ИБ (может быть реализована при помощи *SIEM*-решения);
- подсистему контроля защищенности данных и выявления уязвимостей в доступе к ним (может быть реализована при помощи *DCAP*-решения);
- подсистему контроля информационных потоков и противодействия утечкам защищаемой информации (может быть реализована при помощи *DLP*-решения).

С нашей точки зрения, именно они могут играть роль фундамента, на котором с соблюдением принципа разумной достаточности может быть построено «здание ОИБ» в конкретной организации.

Программные продукты компании «СёрчИнформ», впрочем, как и другие аналогичные, вполне вписываются в рассмотренную модель и позволяют

5 Комплексные системы управления информационной безопасностью [Электронный ресурс] // Rubytech. URL: https://rubytech.ru/products/informatsionnaya-bezopasnost/napravleniya-informatsionnoy-bezopasnosti/kompleksnye-sistemy-upravleniya-informatsionnoy-bezopasnostyu/ (дата обращения: 05.08.24).

6 How to Enhance Your Cybersecurity Platform: XDR vs EDR vs SIEM vs IRM vs SOAR vs DLP [Электронный ресурс] // Apriorit. URL: https://www.apriorit.com/dev-blog/enhancing-cybersecurity-platform-xdr-edr-siem-irm-soar-dlp (дата обращения: 05.08.24).

7 Дудоров И. Системы DCAP: как защитить самое главное [Электронный ресурс] // Anti-malware. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Data-Centric-Audit-and-Protection (дата обращения: 08.08.24).

в полной мере реализовать указанные элементы системы комплексного управления ИБ на уровне организации. В равной степени это касается вопросов недопущения реализации угроз со стороны внутренних нарушителей при помощи *DLP*-системы «КИБ СёрчИнформ»[8], контроля защищенности данных и выявления уязвимостей в доступе к ним путем применения *DCAP*-системы «СёрчИнформ FileAuditor»[9], выявления аномалий в информационных потоках и оповещения о критических событиях в режиме онлайн при помощи *SIEM*-системы «СёрчИнформ SIEM»[10]. Все названные решения легко сочетаются между собой. При совместном использовании они способны обеспечить полномасштабную защиту деятельности организации на всех уровнях.

Противодействие утечкам защищаемой информации

Современные *DLP*-системы, эволюционируя, вбирали в себя наиболее удачные функции [9–12]. Следствием этого стала чрезвычайная их схожесть между собой. Поэтому ниже приведена обобщенная архитектура *DLP*-системы на примере «КИБ СёрчИнформ» (КИБ). В других системах могут быть отличия – работа без баз данных (БД) или выполнение анализа на агенте, а не на сервере.

Источником информации, как правило, являются действия, которые работник совершает, перемещая различные данные. Вся активность пользователя перехватывается условными «сборщиками» (снифферами, сетевыми анализаторами, модулями перехвата). За понятием «сборщик» обычно кроется один или несколько способов перехвата информации: сетевой перехват, перехват путем интеграции со сторонними продуктами [с почтовыми и прокси-серверами], агентский перехват и перехват путем установки *DLP*-системы «в разрыв». В задачи, решаемые «сборщиками» информации, входит и ее парсинг – извлечение структурированной информации из неструктурированных или полуструктурированных данных. Из перехваченных пакетов парсеры извлекают метаданные (дату, время, *IP*-адрес, доменную «учетку» пользователя) и текст (переписки, вложения). Парсеры могут отбрасывать «ненужную» с точки зрения ИБ информацию, например, медиаконтент (картинки, видеофайлы).

Далее информация записывается на хранение в БД. *DLP*-системы в основном используют *SQL*-подобные БД, поскольку они наиболее распространены. Но встречаются решения и на Oracle, PostgreSQL, SQLite. «КИБ СёрчИнформ» использует MSSQL и PostgreSQL.

После записи информации в БД с ней уже можно работать – делать запросы и анализировать выдачу. Однако, БД не оптимизированы для быстрого поиска текстовой информации. А основная информация, перехватываемая и обрабатываемая *DLP*-системами, – именно текст. В контексте решения описываемых задач для превращения «сырых» данных в оптимизированные для быстрого поиска структуры используется индексация. Индекс содержит информацию о слове, которое нужно найти (где оно встречается, какая у него позиция в документе относительно других слов и т.д.).

После индексации по перехваченной информации можно проводить быстрый поиск. В любой *DLP*-системе для анализа используются три типа средств: «просмотрщик», средство автоматизации, средство отчетности. «Просмотрщик» обеспечивает выполнение ручного поиска (например, при расследовании инцидентов, проверке правил, по которым *DLP*-система будет автоматически (по расписанию) проверять перехваченную информацию и т.п.). Средство автоматизации предназначено для автоматизации проверок в *DLP*-системе: специалист по ИБ создает правило, в котором указывает что, где и как часто нужно искать (формируется расписание) и кого уведомлять в случае нарушения политики. Средство отчётности нужно для предоставления информации о возможных нарушениях в той или иной форме.

Реальная архитектура «КИБ СёрчИнформ» значительно сложнее по сравнению со схематичными связями, описанными выше. Информацию с компьютера сотрудника перехватывают платформы NetworkController и EndpointController. Первая отвечает за сетевой перехват, вторая – за агентский (рис. 2). Возможности сетевой платформы могут быть расширены за счет перехвата путем интеграции (количество каналов перехвата не увеличивается, но появляется возможность перехвата шифрованных данных). Когда информация записана в БД MSSQL, к ее обработке приступает SearchServer. С помощью этого «движка» из информации, которая содержит текст, формируются индексы. При этом информация, которая изначально не содержит текст, индексацию не проходит и доступна для поиска в виде БД. Все компоненты КИБ имеют клиент-серверную архитектуру. Серверную часть представляет одна из платформ для перехвата данных, клиентскую – приложения для поиска и просмотра перехваченных данных в ходе проведения служебных расследований.

Модули перехвата, которые входят в состав системы, обеспечивают возможность контроля практически всех популярных каналов обмена информацией (рис. 3).

8 СёрчИнформ КИБ [Электронный ресурс] // SearchInform. URL: https://searchinform.ru/products/kib/ (дата обращения: 05.08.24).

9 СёрчИнформ FileAuditor [Электронный ресурс] // SearchInform. URL: https://searchinform.ru/products/fileauditor/ (дата обращения: 05.08.24).

10 СёрчИнформ SIEM [Электронный ресурс] // SearchInform. URL: https://searchinform.ru/products/siem/ (дата обращения: 05.08.24).

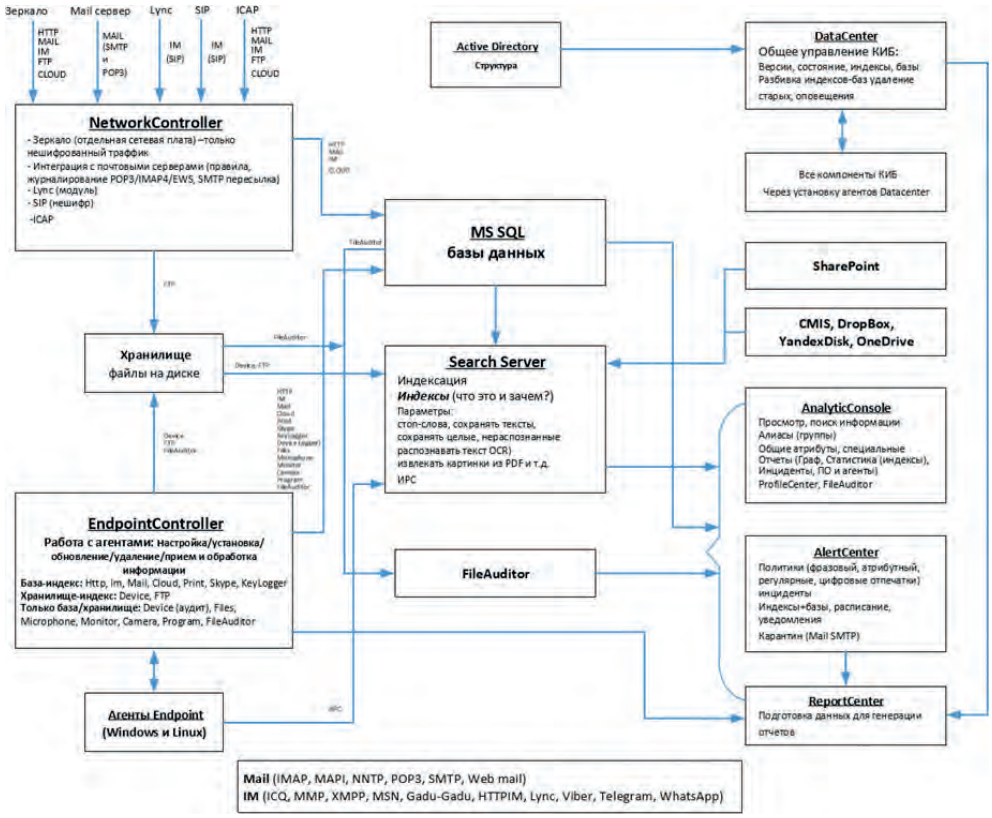

Рис. 2. Взаимодействие компонентов «КИБ СёрчИнформ»

КИБ разработан с учетом специфики работы крупных компаний. Основные достоинства системы:

- *Наиболее полный контроль информационных потоков.* КИБ контролирует все критичные для бизнеса каналы коммуникаций – Exchange, Lync, Skype, корпоративную телефонию, файловые сервера, Sharepoint, Office365, Cisco Messenger, Telegram, Zoom, Viber, WhatsApp, Slack, веб-почту, облачные хранилища, социальные сети, блоги, форумы. Комплексный контроль сетевых каналов делает возможным их безопасное использование. Отсутствие блокировок позитивно сказывается на бизнес-процессах и повышает эффективность коммуникации сотрудников;
- *Продвинутые технологии анализа.* Помимо «классических» технологий анализа (морфология, словари, регулярные выражения, цифровые отпечатки, OCR), в КИБ включены и собственные разработки компании, повышающие эффективность системы. Например, детектирование текстов, близких по смыслу или содержанию к эталонным. Поиск изображений, визуально похожих на эталон. Поиск по любым аудиозаписям (технология преобразования аудио в текст) и контентный поиск по видеозаписи действий пользователя (можно просматривать видео только интересующих действий, например, работы с конфиденциальным документом). Есть возможность построения контентных маршрутов для любых перехваченных файлов, а также профилирование пользователей на основе перехвата их переписок;
- *Качественные средства расследования.* КИБ дает службе ИБ средства для проведения детального наблюдения – позволяет делать аудио- и видеозапись действий пользователя, фиксировать любые

Рис. 3. Модули перехвата «КИБ Сёрчинформ»

его действия с файлами или папками, журналами регистрации событий (логами), устройствами, ПО. Также доступно аудио- и видеонаблюдение за нарушителями в реальном времени. Это помогает в расследовании инцидентов – *DLP*-система позволяет в точности воспроизвести нарушение и установить круг причастных лиц, что отсутствует во многих аналогичных системах и не позволяет полноценно разобраться в контексте нарушения. Также присутствуют средства журналирования действий сотрудников ИБ-службы в консолях AlertCenter, AnalyticConsole, DataCenter, EndpointController, NetworkController, *SIEM*. Тем самым снимается вопрос «кто будет контролировать контролеров». Эти журналы нельзя отредактировать;

- *Универсальное средство защиты информации.* КИБ работает как полноценная *DLP*-система, а также предоставляет дополнительные средства для ОИБ. В нее встроены, например, шифрование записываемых на внешний носитель документов, разграничение доступа к файловой системе, полноценный контроль терминальных серверов, аудит оборудования и ПО. Кроме того, КИБ может выступать как обработчиком информации, так и источником, что открывает широкие возможности по интеграции с другими системами;
- *Возможность контроля продуктивности пользователей в приложениях и на сайтах.* Она расширяет область применения *DLP*-систем, помогая повысить уровень общей дисциплины в компании, определить слабые места в бизнес-процессах. Это избавляет заказчика от необходимости закупать и сопровождать две различные системы с пересекающимися задачами и устанавливать два различных агентских модуля на каждый персональный компьютер (ПК) – все доступно в одном решении;
- *Продвинутые функции агента.* Агент *DLP*-системы «вычитывает» информацию об устройствах на ПК (видеоадаптеры, запоминающие устройства, мониторы и др.) и установленных программах, а затем сообщает службе ИБ об изменениях в конфигурации компьютеров. Помимо этого, агент выявляет сторонние программы контроля и *DLP*-системы на компьютерах пользователей;
- *Профайлинг.* Эта уникальная система компании «СёрчИнформ» автоматически анализирует переписку сотрудника в почте, мессенджерах и соцсетях и составляет его психологический портрет. Профайлинг указывает на сильные и слабые стороны сотрудника, находит точки давления, определяет склонность к преступлениям (с указанием, к каким именно);
- *Отслеживание и визуализация связей между сотрудниками.* Интерактивный граф отношений даёт наглядное представление о круге общения и контактах по основным каналам коммуникаций внутри компании и с внешними адресатами;
- *Разграничение прав доступа к информации.* Мощная ролевая модель дает возможность гибкой настройки прав доступа к перехваченной информации;
- *Наличие продуктов компании в реестре отечественного ПО.* КИБ имеет сертификат ФСТЭК по уровню доверия 4 (запись в реестре под № 4144). Средства защиты информации, соответствующие 4 уровню доверия, подлежат применению в значимых объектах КИИ 1 категории, в государственных информационных системах (ИС) 1 класса защищенности, в автоматизированных системах управления производственными и технологическими процессами (АСУ ТП) 1 класса защищенности, в информационных системах (ИС) персональных данных (ПДн) при необходимости обеспечения 1 уровня защищенности ПДн, в ИС общего пользования 2 класса[11].

Контроль защищенности данных и выявления уязвимостей в доступе к ним

Решения класса *DCAP* предназначены для обнаружения, категоризации и защиты структурированных, неструктурированных и полуструктурированных данных. Речь идет об информации на ПК сотрудников, а также той, что разбросана по сетевым папкам, облачным хранилищам, БД и т.д. Реальная ситуация, когда все учтено и находится под контролем, характеризуется тем, что критичные данные не содержатся в единой базе, видоизменяются в каждой БД по-своему, а по пути еще и сохраняются пользователями на персональных устройствах, в облаках и общедоступных папках. В результате персональные, платежные, учетные данные, файлы с коммерческой тайной, чертежи и прочие технические документы бесконтрольно множатся, что создает как бизнес-риски, так и риски ИБ. *DCAP*-решения появились как ответ на описанные проблемы.

Несмотря на различия в функционале, *DCAP*-системы в «базовой» комплектации должны выполнять следующие функции:

- обнаруживать и классифицировать данные;
- проводить мониторинг прав доступа;
- отслеживать операции с данными;
- обеспечивать защиту данных, запрещая нежелательные операции с ними.

Успеху DCAP в значительной степени способствовало принятие законов о защите ПДн: регуляторы

11 Сертификаты и лицензии [Электронный ресурс] // SearchInform. URL: https://searchinform.ru/docs/ (дата обращения: 05.08.24).

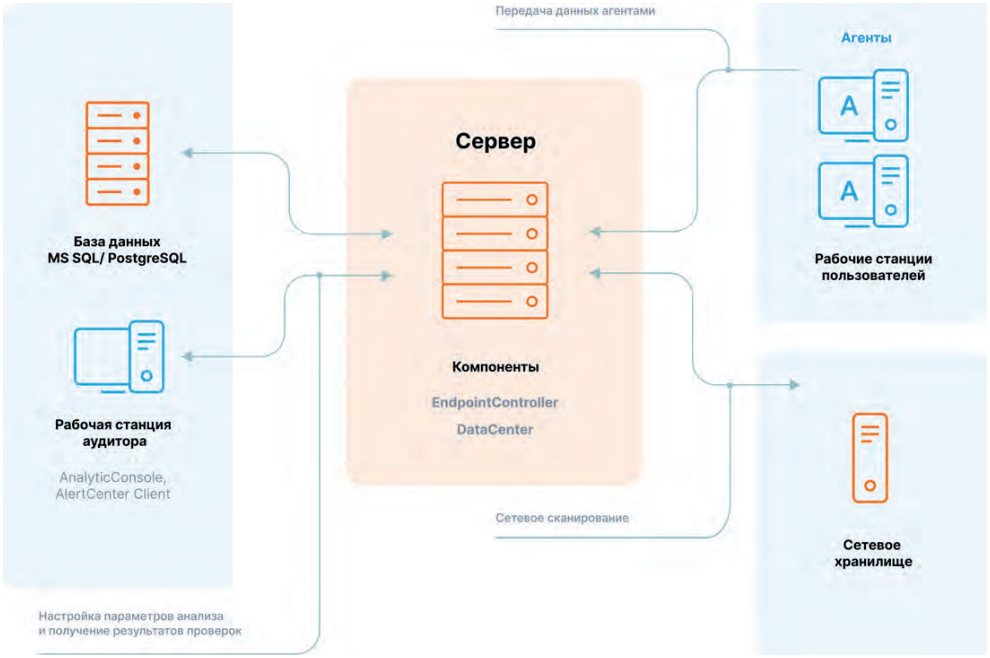

Рис. 4. Схема работы «FileAuditor»

твердо обозначили намерение жестко наказывать за утечку, справедливо считая, что вовремя обнаруженная «бесхозная» либо общедоступная информация позволяет избежать больших проблем. Первой среди отечественных разработчиков свое *DCAP*-решение «FileAuditor» выпустила компания Сёрч-Информ в 2019 г.

«FileAuditor» решает следующие задачи:

- *Классификация данных.* Позволяет выделить из общего документооборота информацию, подлежащую защите, и определить ее ценность. Структурированные данные легче защитить: для каждой группы данных (например, финансовая информация, ноу-хау) в «FileAuditor» можно разработать отдельный набор правил в соответствии с внутренними политиками ИБ и требованиями регуляторов;
- *Защита данных.* Программа проводит регулярный аудит мест хранения и обнаруживает конфиденциальные документы в любом месте корпоративной ИС – на ПК сотрудников, в сетевых папках и на файловых серверах;
- *Аудит доступа к данным.* Бизнес-информация становится уязвимой, когда ею делятся. Чем больше людей имеют доступ к данным, тем выше риск потерять ценные сведения. «FileAuditor» позволяет отслеживать группы сотрудников, которые создают, хранят или обрабатывают данные ограниченного доступа;
- *Контроль за действиями пользователей.* «FileAuditor» следит за тем, какие операции с конфиденциальными данными совершают пользователи и сверяется с политикой ИБ. Например, систему насторожит удаление критичных данных, перемещение конфиденциальных документов в общедоступные папки.

ИБ-специалист может задать для поиска документов конкретный текст, атрибут, директории, компьютер или их сочетание, что позволяет контролировать в первую очередь критичные данные.

Как уже было сказано, «FileAuditor» позволяет отслеживать наличие критичной информации на компьютерах пользователей и права доступа к файлам. Сканирование ресурсов согласно настроенным правилам, предоставление дерева папок/файлов, а также прав доступа к ним может осуществляться либо с помощью агента, либо с помощью службы анализа данных на сервере (рис. 4). Стоит упомянуть, что на агенте используется облегченная версия поискового «движка» – miniSearchServer, что приводит к ограничению аналитических функций (например, нет возможности распознавать текст из картинок, используются не все поддерживаемые типы поиска, а лишь некоторые из них и т.д.). С другой стороны, таким способом обеспечивается компромисс между скоростью, гибкостью и объемом потребных ресурсов.

Особого внимания заслуживает интеграция «FileAuditor» с КИБ, что позволяет автоматизировать выполнение ряда задач. Например, в «FileAuditor» можно настроить правило на поиск новых важных документов. Результаты поиска или аудита отображаются на отдельной вкладке приложения «Консоль аналитика». ИБ-специалист получает наглядную информацию – тип найденного файла в общей классификации и правило, под действие которого попадает данный файл и т.д. (рис. 5).

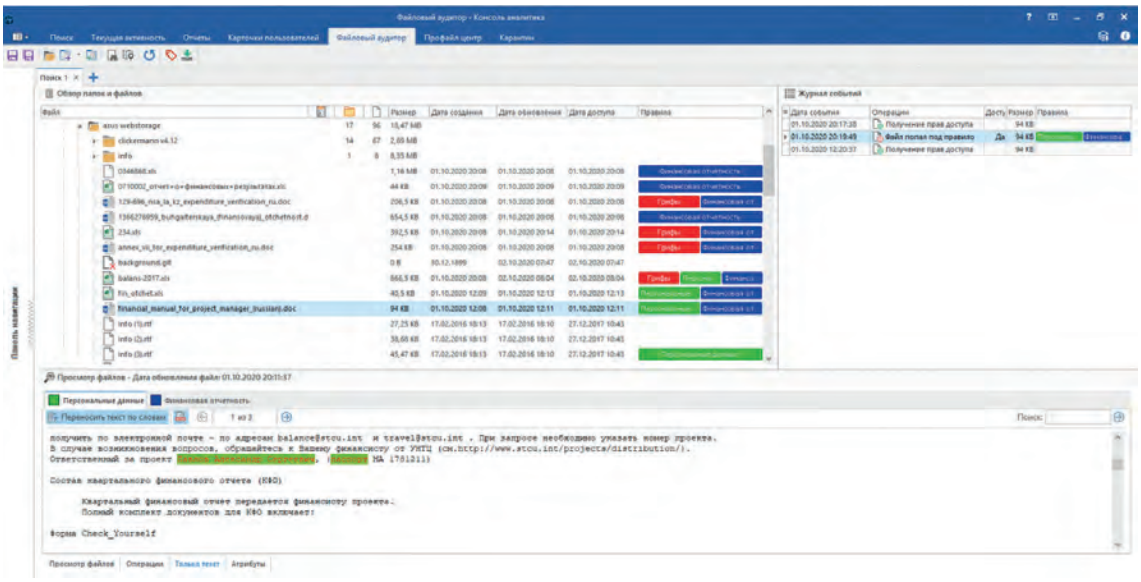

Рис. 5. «FileAuditor»: результаты поиска

Кроме того, «FileAuditor» позволяет практически мгновенно узнать, где лежат важные для организации документы, чтобы убедиться, что доступ к этим данным имеют только те сотрудники, которые в нем нуждаются (рис. 6).

А с помощью приложения AlertCenter можно оперативно получать соответствующие уведомления.

Управление событиями ИБ

В целом задача *SIEM*-систем – попытаться представить сетевую активность в удобном для восприятия виде. Эти системы появились как результат комбинации двух видов решений: *SIM* (*Security Information Management*) – управление информацией о безопасности и *SEM* (*Security Event Management*) – управление событиями безопасности. В общем случае *SIEM*-система призвана собирать, анализировать и представлять информацию из сетевых устройств и средств ОИБ. Также в эту систему должны входить приложения для управления идентификацией и доступом, уязвимостями приложений и БД. Как правило, *SIEM*-система реализует следующие функции: отправку предупреждений на основе предопределенных настроек, формирование отчетов и логирование для упрощения мониторинга ИБ, просмотр данных на разных уровнях детализации. Для этого *SIEM*-система собирает логи разных приложений, обрабатывает и кладет их в централизованное хранилище,

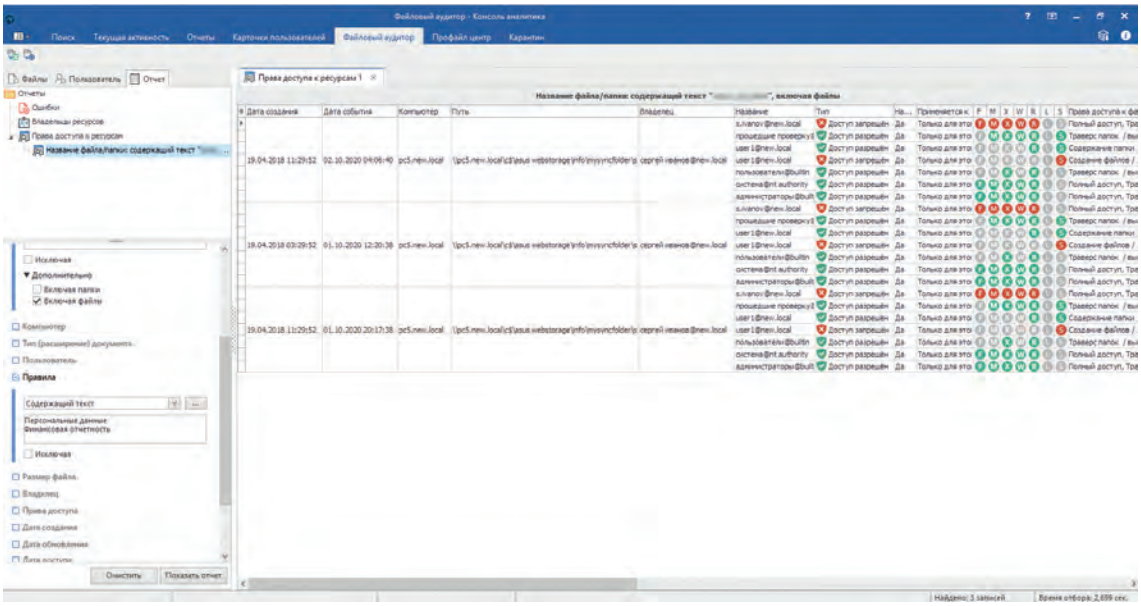

Рис. 6. «FileAuditor»: права доступа

DOI: 10.21681/2311-3456-2024-5-67-78

с которым удобно работать. Использование *SIEM*-системы позволяет увидеть более полную картину активности сети и события ИБ. В том числе и тогда, когда обычные средства обнаружения по отдельности не видят атаки, но она может быть обнаружена при тщательном анализе и корреляции информации из различных источников [13–15].

К типовым сценариям использования *SIEM*-системы можно отнести:

- отслеживание аутентификации и обнаружение компрометации учетных записей (аккаунтов) пользователей и администраторов;
- отслеживание случаев заражения и обнаружение вредоносного ПО;
- мониторинг подозрительного исходящего трафика и передаваемых по сети данных, обнаружение кражи данных и других подозрительных внешних соединений;
- отслеживание системных изменений и других административных действий во внутренних системах и их соответствия разрешенной политике ИБ;
- отслеживание атак на веб-приложения и их последствий, обнаружение попыток компрометации веб-приложений путем анализа разных отчетов.

«СёрчИнформ SIEM» представляет собой решение, предназначенное для сбора и автоматического анализа событий из различных корпоративных систем для выявления угроз и нарушений политик ИБ [15]. Источниками событий могут быть журналы контроллеров доменов, БД агентов «Сёрчинформ КИБ», сетевое оборудование, ПО и др. Система отслеживает события и автоматически, по настроенным правилам, выявляет потенциально опасные связи и цепочки таких событий. Правила анализа и формирования взаимосвязей между событиями предустановлены в систему, их остается только настроить «под себя».

Сбор данных для *SIEM*-системы, а также их нормализация и первоначальный анализ осуществляется в реальном времени с помощью коннекторов, обеспечивающих связь со всеми компонентами информационной инфраструктуры (рис. 7). Коннекторы собирают и анализируют события из различных источников данных. Например, WinEventConnector собирает и анализирует логи контроллеров домена, KavEventConnector подключается к БД Kaspersky Security Center и читает записи в ней, CiscoConnector собирает события сетевых устройств Cisco.

Коннекторы «СёрчИнформ SIEM» можно условно разделить на три группы:

1) сами собирающие события путем подключения к логам, журналам или базам источников данных (WinEventConnector, KAVConnector, ExchangeConnector и др.);
2) получающие события Syslog из различных аппаратных устройств или приложений (SyslogConnector, NetFlowConnector, LinuxConnector, CiscoConnector и др.);
3) собирающие события от установленного агента *SIEM*-системы (1CConnector, CWAConnector).

В БД «СёрчИнформ SIEM» под управлением СУБД MongoDB хранятся все события и инциденты, которые подпадают под заданные правила. Создание БД является необходимым условием для корректной работы *SIEM*-системы, независимо от перечня используемых коннекторов.

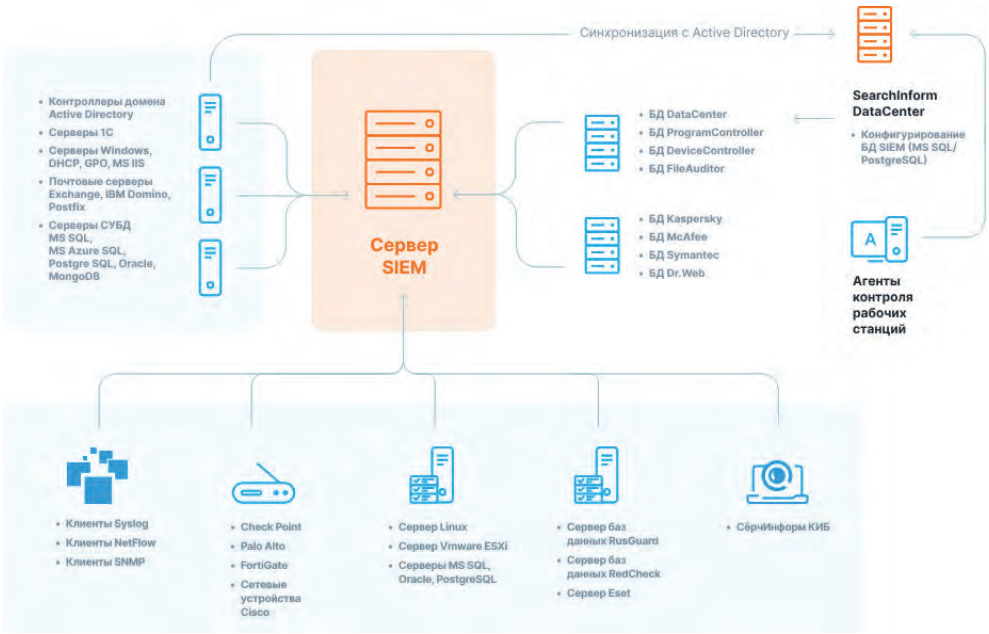

Рис. 7. Схема работы «СёрчИнформ SIEM»

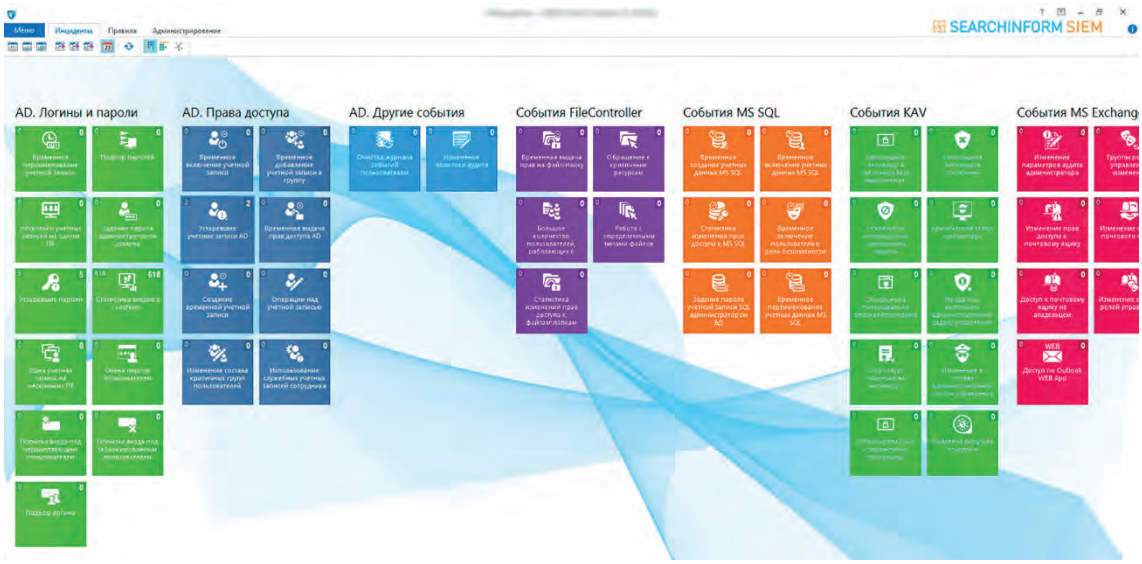

Рис. 8. «СёрчИнформ SIEM»: экран отображения инцидентов (правила визуализируются в виде плиток)

Сканер сети осуществляет сканирование локального сегмента корпоративной сети по заданным настройкам, в результате чего создается «слепок» объектов, который может использоваться для мониторинга, анализа и помощи в администрировании этой сети.

Для отображения связей объектов сети (компьютеров и пользователей), а также количества успешных/неуспешных подключений пользователей к компьютерам используется карта подключений. Она представляет собой граф, формируемый на основе событий по правилу «Статистика входов в систему» (WinEventConnector).

Правила *SIEM*-системы – набор параметров, которые определяют взаимосвязь между событиями, а также относят события к категории инцидентов ИБ (рис. 8). Между событиями и инцидентами ИБ есть отличия, причем события могут быть одинаковыми для всех организаций, а инциденты – только то, что сама организация таковыми посчитает. Например, событием считается каждый сеанс ввода пароля, а инцидентом ИБ – ввод пароля как минимум пять раз подряд за минуту. В системе есть предустановленные шаблоны правил по каждому коннектору, на основании которых можно создавать пользовательские правила.

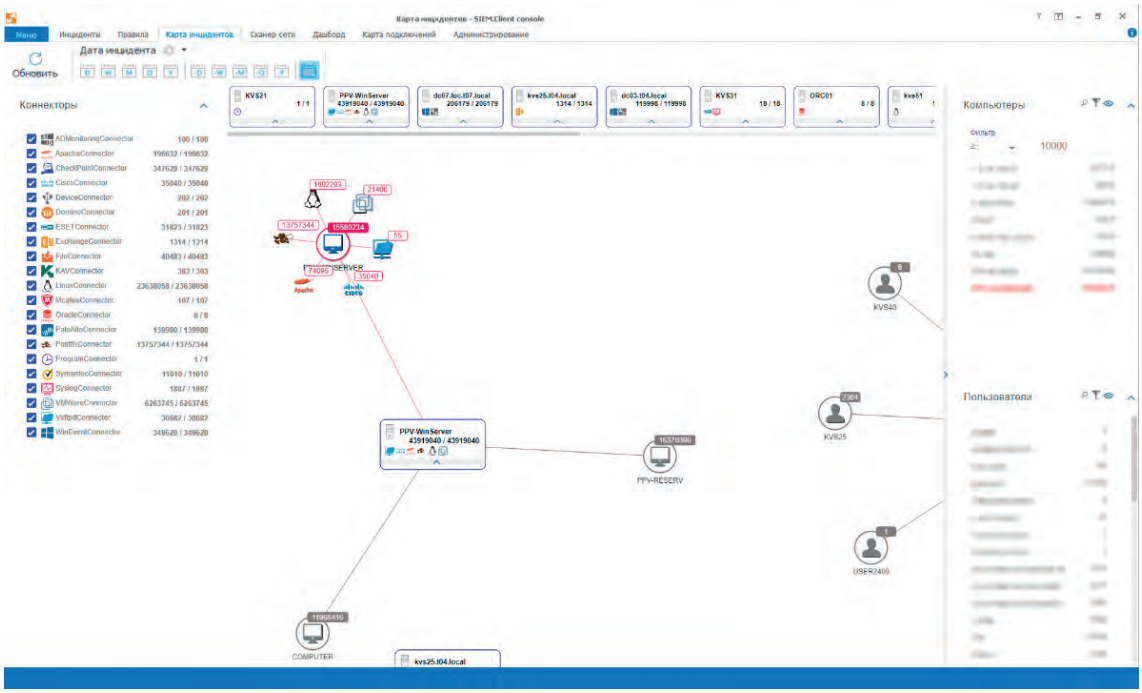

Рис. 9. «СёрчИнформ SIEM»: карта инцидентов

DOI: 10.21681/2311-3456-2024-5-67-78

Кросс-корреляцией называется перекрестное выявление зависимостей/корреляций между данными из разных источников, что позволяет более широко использовать возможности *SIEM*-системы, выявляя атаки и неполадки в сети по комплексным признакам. При помощи сервиса кросс-корреляции в «Сёрч-Информ SIEM» пользователь может сам создать необходимые ему правила на основании сопоставления событий из нескольких источников.

Карта инцидентов – граф, который интерпретирует структуру сети и объектов в ней (компьютеров и пользователей) в привязке к серверам с установленными коннекторами. На одноименной вкладке отображается общее количество инцидентов ИБ по каждому коннектору для определенного пользователя/компьютера (рис. 9). События на графе отображаются постепенно, порциями по 100 000; их можно детализировать.

Для отображения данных, собранных системой, в удобном формате, упрощения их анализа, отслеживания тенденций событий используется инфопанель «Дашборд» – панель ключевых показателей. На соответствующую вкладку можно добавить неограниченное количество виджетов. Каждый новый виджет создается на основе базового, но может иметь индивидуальные настройки (определенный набор пользователей, компьютеров, коннекторов и др.). По умолчанию имеется 12 базовых виджетов:

- топ дат по количеству событий;
- топ пользователей по количеству событий;
- копирование файлов на съемные устройства;
- события Syslog;
- использование учетных записей;
- обнаружение вирусов на ПК (Kaspersky Internet Security);
- обнаружение вирусов на ПК (SymantecEndpoint-Protection);
- обнаружение вирусов на ПК (McAfeeInternetSecurity);
- обнаружение вирусов на ПК (EsetSmartSecurity);
- обнаружение вирусов на ПК (Dr. Web);
- количество событий по датам;
- попытки входа.

С учетом всего вышесказанного многие организации рассматривают использование *SIEM*-системы в качестве дополнительного и очень важного элемента защиты от целенаправленных атак.

Выводы

С увеличением числа кибератак в ситуации растущей геополитической нестабильности становится ясно, что на сегодняшний день эффективное управление инцидентами ИБ превратилось в обязательную составляющую защиты информационно-технологических систем компаний самого различного масштаба. По результатам проведенного анализа содержания и роли процессов ОИБ в эффективной работе современных ИС следует сделать вывод о том, что для мониторинга событий, обнаружения угроз, соответствия требованиям и автоматизации процессов безопасности оптимальным набором характеристик обладает комплексное решение, интегрирующее в себе функционал *SIEM*-, *DCAP*- и *DLP*-систем.

Совместное использование рассмотренных в статье в качестве примера продуктов «СёрчИнформ SIEM», *DLP* «СёрчИнформ КИБ» и *DCAP* «FileAuditor» повышает уровень ИБ организации. *SIEM*-система выявляет аномальное поведение и определяет способ получения доступа к информации. *DLP*-система оценивает содержимое всех коммуникаций. *DCAP*-система отслеживает действия с данными, запрещая нежелательные операции. Высокоинтегрированная связка данных систем дает возможность максимально полно расследовать нарушения ИБ и собрать необходимую доказательную базу.

Комплексные системы защиты информации наиболее востребованы в государственных структурах, которые из-за специфики закупок с большей охотой приобретут одну интегрированную систему, чем несколько продуктов разного класса, назначения и, к тому же, предлагаемых разными вендорами. Проведенные исследования позволяют дать практические рекомендации для эффективного ОИБ и показывают, что предлагаемые подходы к управлению ИБ обеспечат поддержание требуемого уровня защищенности ИС предприятия в условиях динамически изменяющихся и развивающихся угроз.

Литература

1. *Страхов А. А., Дубинина Н. М. Об утечке данных и DLP-системах // Криминологический журнал. 2022. № 4. С. 226–232. DOI: 10.24412/2687-0185-2022-4-226-232.*
2. *Страхов А. А., Дубинина Н. М. О безопасности персональных данных // Криминологический журнал. 2024. № 1. С. 255–263. DOI: 10.24412/2687-0185-2024-1-255-263.*
3. *Токарев М. Н., Вершинин А. Н. Импортозамещение программного обеспечения // Международный журнал гуманитарных и естественных наук. 2023. № 6-3 (81). С. 156–162. DOI: 10.24412/2500-1000-2023-6-3-156-162.*
4. *Федоров А. В., Жихарев А. Г., Кальченко Д. М. Обеспечение информационной безопасности в органах исполнительной власти. Проблемы и решения // Научный результат. Информационные технологии. 2024. Т. 9, №1. С. 19-28. DOI: 10.18413/2518-1092-2024-9-1-0-3.*
5. *Полтавцева М. А. Модель активного мониторинга как основа управления безопасностью промышленных киберфизических систем // Вопросы кибербезопасности. 2021. № 2(42). С. 51-60. DOI: 10.21681/2311-3456-2021-2-51-60.*

6. Сизов В. А., Киров А. Д. Проблемы внедрения SIEM-систем в практику управления информационной безопасностью субъектов экономической деятельности // Открытое образование. 2020. Т. 24. № 1. С. 69–79. DOI: 10.21686/1818-4243-2020-1-69-79.
7. Сунаева Г. Г., Петрова К. А. Внедрение комплаенс-контроля в условиях цифровизации экономики // Вестник УГНТУ. Наука, образование, экономика. Серия экономика. № 2 (40), 2022. С. 16–23. DOI: 10.17122/2541-8904-2022-2-40-16-23.
8. Алексеев А. В., Куприянов Д. О., Стефанович И. Д., Заведеев Ю. М. Анализ интеллектуальных технологий управления ИБ морских интегрированных автоматизированных систем // Труды Крыловского государственного научного центра. 2021. № S1. С. 196–198. DOI: 10.24937/2542-2324-2021-1-S-I-196-198.
9. Morozov V., Miloslavskaya N. DLP Systems as a Modern Information Security Control. In: Samsonovich A., Klimov V. (eds) Biologically Inspired Cognitive Architectures (BICA) for Young Scientists. BICA 2017. Advances in Intelligent Systems and Computing, 2018 Vol. 636, Q4 pp. 296–301. DOI: 10.1007/978-3-319-63940-6_42
10. Зарубин А. В., Смирнов М. Б., Харитонов С. В., Денисов Д.В. Основные драйверы и тенденции развития DLP-систем в Российской Федерации // Прикладная информатика. 2020. Т. 15. № 3. С. 75–90. DOI: 10.377 91/2687-0649-2020-15-3-75-90.
11. Ying, Z., Wu, B. DLP: towards active defense against backdoor attacks with decoupled learning process. Cybersecurity 6, 9 (2023). DOI: 10.1186/s42400-023-00141-4.
12. Попугаева В. А., Шарыпова Т. Н. Особенности рынка DLP-систем // Colloquium-Journal. 2022. № 12-1 (135). С. 32–33. DOI: 10.24412/2520-6990-2022-12135-32-33.
13. Милославская Н. Г. Научные основы построения центров управления сетевой безопасностью в информационно-телекоммуникационных сетях / М.: Горячая линия – Телеком, 2021. – 432 с.
14. Кирсанов Д. Г., Айдинян А. Р. Эффективное обеспечение безопасности с помощью SIEM // Молодой исследователь Дона. 2024. № 9(3). С. 45–49.
15. Аникин И. В., Чепайкин Р. Н. Автоматизация процесса трансляции корреляционных правил для систем SIEM // Научные труды КубГТУ. 2023. № 4. С. 76–87.

COMPREHENSIVE SOLUTIONS TO MINIMISE INTERNAL INFORMATION SECURITY THREATS

Morozov V. E.[12], Miloslavskaya N. G.[13]

Purpose of work: *determination of the composition of modern solutions, which together allow creating a system of complex organization's information security management.*

Research methods: *analysis of relevant scientific publications, conceptual modelling, expert evaluation, synthesis of the system of complex information security managementf.*

Results obtained: *The article details the components of the information security (IS) management process and discusses the possible composition of a complex IS management system for an organisation focused on minimising internal threats. It is shown that such a system should include the following key elements: a subsystem of centralised monitoring of events and investigation of IS incidents, subsystem of data security control and identification of data access vulnerabilities, as well as a subsystem of control of data flows and counteraction to protected data breaches. These elements can be implemented by SIEM, DCAP and DLP systems, respectively. The main concepts and technologies on the basis of which these systems are developed, their architecture, features and analytical capabilities are considered using the example of software developed by the SearchInform company (SearchInform SIEM, SearchInform FileAuditor and SearchInform KIB). The analysis of all characteristics and experience in the use of these systems (provided they are integrated) shows that they can provide full-scale corporate protection at all levels.*

Practical significance *consists in substantiating the sufficiency of the specified composition of the IS management system to solve the problem of minimising internal threats.*

Keywords: *DLP, DCAP, SIEM, internal information security threats, information security incident, monitoring, information security event, information security management.*

References

1. Strakhov A. A., Dubinina N. M. Ob utechke dannykh i DLP-sistemakh // Kriminologicheskiy zhurnal. 2022. № 4. S. 226-232. DOI: 10.24412/2687-0185-2022-4-226-232.
2. Strakhov A. A., Dubinina N. M. O bezopasnosti personal'nykh dannykh // Kriminologicheskiy zhurnal. 2024. № 1. S. 255–263. DOI: 10.24412/2687-0185-2024-1-255-263.
3. Tokarev M. N., Vershinin A. N. Importozameshcheniye programmnogo obespecheniya // Mezhdunarodnyy zhurnal gumanitarnykh i yestestvennykh nauk. 2023. № 6-3 (81). S. 156–162. DOI: 10.24412/2500-1000-2023-6-3-156-162.
4. Fedorov A. V., Zhikharev A. G., Kal'chenko D. M. Obespecheniye informatsionnoy bezopasnosti v organakh ispolnitel'noy vlasti. Problemy i resheniya // Nauchnyy rezul'tat. Informatsionnyye tekhnologii. 2024. T. 9, №1. S. 19-28. DOI: 10.18413/2518-1092-2024-9-1-0-3.

12 Victor E. Morozov, Ph.D Associate Professor, Specialist of LLC «Librasoft», Minsk, Belarus. E-mail: v.morozov@searchinform.ru
13 Natalia G. Miloslavskaya, Dr.Sc., Ph.D in Cybersecurity, Associate Professor, Professor Dep. of Information Security of Banking Systems of National Research Nuclear University MEPhI, Moscow, Russia. E-mail: NGMiloslavskaya@mephi.ru

5. *Poltavtseva M. A. Model' aktivnogo monitoringa kak osnova upravleniya bezopasnost'yu promyshlennykh kiberfizicheskikh sistem // Voprosy kiberbezopasnosti. 2021. № 2(42). S. 51–60. DOI: 10.21681/2311-3456-2021-2-51-60.*
6. *Sizov V. A., Kirov A. D. Problemy vnedreniya SIEM-sistem v praktiku upravleniya informatsionnoy bezopasnost'yu sub"yektov ekonomicheskoy deyatel'nosti // Otkrytoye obrazovaniye. 2020. T. 24. № 1. S. 69–79. DOI: 10.21686/1818-4243-2020-1-69-79.*
7. *Sunayeva G. G., Petrova K. A. Vnedreniye komplayens-kontrolya V usloviyakh tsifrovizatsii ekonomiki // Vestnik UGNTU. Nauka, obrazovaniye, ekonomika. Seriya ekonomika. № 2 (40), 2022. S. 16–23. DOI: 10.17122/2541-8904-2022-2-40-16-23.*
8. *Alekseyev A. V., Kupriyanov D. O., Stefanovich I. D., Zavedeyev YU. M. Analiz intellektual'nykh tekhnologiy upravleniya IB morskikh integrirovannykh avtomatizirovannykh sistem // Trudy Krylovskogo gosudarstvennogo nauchnogo tsentra. 2021. № S1. S. 196–198. DOI: 10.24937/2542-2324-2021-1-S-I-196-198.*
9. *Morozov V., Miloslavskaya N. DLP Systems as a Modern Information Security Control. In: Samsonovich A., Klimov V. (eds) Biologically Inspired Cognitive Architectures (BICA) for Young Scientists. BICA 2017. Advances in Intelligent Systems and Computing, 2018 Vol. 636, Q4 pp. 296–301. DOI: 10.1007/978-3-319-63940-6_42*
10. *Zarubin A. V., Smirnov M. B., Kharitonov S. V., Denisov D.V. Osnovnyye drayvery i tendentsii razvitiya DLP-sistem v Rossiyskoy Federatsii // Prikladnaya informatika. 2020. T. 15. № 3. S. 75–90. DOI: 10.377 91/2687-0649-2020-15-3-75-90.*
11. *Ying, Z., Wu, B. DLP: towards active defense against backdoor attacks with decoupled learning process. Cybersecurity 6, 9 (2023). DOI: 10.1186/s42400-023-00141-4.*
12. *Popugayeva V. A., Sharypova T. N. Osobennosti rynka DLP-sistem // Colloquium-Journal. 2022. № 12-1 (135). S. 32–33. DOI: 10.24412/2520-6990-2022-12135-32-33.*
13. *Miloslavskaya N. G. Nauchnyye osnovy postroyeniya tsentrov upravleniya setevoy bezopasnost'yu v informatsionno-telekommunikatsionnykh setyakh / M.: Goryachaya liniya – Telekom, 2021. – 432 s.*
14. *Kirsanov D. G., Aydinyan A. R. Effektivnoye obespecheniye bezopasnosti s pomoshch'yu SIEM // Molodoy issledovatel' Dona. 2024. № 9(3). S. 45-49.*
15. *Anikin I. V., Chepaykin R. N. Avtomatizatsiya protsessa translyatsii korrelyatsionnykh pravil dlya sistem SIEM // Nauchnyye trudy KubGTU. 2023. № 4. C. 76–87.*