УДК 004.056

ОБЕСПЕЧЕНИЕ НЕПРЕРЫВНОСТИ ФУНКЦИОНИРОВАНИЯ DLP-СИСТЕМЫ В СЛУЧАЕ АВАРИЙНОЙ СИТУАЦИИ В ТЕРРИТОРИАЛЬНО РАСПРЕДЕЛЁННЫХ ЦОД

В.Ю. Семилеткин
Студент группы М22-508 НИЯУ МИФИ, svu_2017@mail.ru

Аннотация. Представлены результаты исследования методов обеспечения непрерывности функционирования DLP-системы в территориально распределённых (ТР) центрах обработки данных (ЦОД). Показано, что существующая зависимость организаций всех форм собственности от информационных технологий (ИТ) повышает их уязвимость к различным угрозам, включая угрозы экстремизма и терроризма. Обоснован выбор отечественных средств виртуализации. Рассчитаны основные показатели надежности для системы, включающей ПК СВ «Брест» и DLP-систему «СёрчИнформ КИБ». На примере «СёрчИнформ КИБ» рассмотрены особенности функционирования DLP-системы при ее развертывании на облачной платформе. Приведены результаты оценки эффективности разработанных политик и поисковых критериев для DLP-системы, ориентированных на выявление случаев распространения материалов, содержащих призывы к экстремизму и терроризму. Сделан вывод, что надежное и непрерывное функционирование DLP-системы существенно снижает вероятность утечек информации и других инцидентов информационной безопасности.

Ключевые слова: информационные системы, информационная безопасность, киберпространство, терроризм, территориально-распределенные ЦОД, экстремизм, DLP-системы.

Введение

Вопросы обеспечения безопасности информационных систем (ИС) играют все более возрастающую роль в современной экономике и управлении. Стабильность работы этих систем имеет решающее значение для устойчивого роста организаций всех форм собственности. Усиливающаяся зависимость и бизнеса, и государственных учреждений от ИТ повышает их уязвимость к различным угрозам, включая угрозы экстремизма и терроризма [1-3]. Данные обстоятельства диктуют необходимость разработки более совершенных методов защиты данных и обеспечения непрерывного функционирования ИС отечественных компаний.

Важнейшей задачей, решение которой необходимо для обеспечения ИБ, является предотвращение утечек конфиденциальной информации. Одним из наиболее эффективных технических средств, позволяющих бороться с утечками, служат DLP-системы [4, 5]. Они помогают контролировать и фильтровать данные, проходящие через сети организации, а также обнаруживают и блокируют несанкционированные попытки передачи важной

и критической информации. Эффективное применение DLP-систем способствует не только предотвращению атак, но и снижению потенциального ущерба от различных инцидентов, уменьшая риски для руководства и сотрудников. В этой связи особое значение приобретает обеспечение защиты и непрерывности работы подобных решений в особенности на фоне угрозы терактов, которые могут привести к серьезным нарушениям в работе ключевых ИС.

Для усиления защиты и повышения устойчивости к внешним угрозам наиболее адекватными мерами на сегодняшний день являются использование возможностей ТР ЦОД и внедрение средств виртуализации. ЦОД – отказоустойчивые решения, которые призваны обеспечить непрерывную работу корпоративных приложений, сервисов и сайтов практически в любых условиях. В свою очередь виртуализация играет важную роль в повышении гибкости и эффективности ИТ-инфраструктуры современных предприятий. Она позволяет значительно увеличить загрузку аппаратных мощностей, улучшает управление ИТ-затратами и упрощает контроль над информацией и приложениями.

В статье обосновывается использование средств виртуализации для обеспечения бесперебойного функционирования DLP-системы (на примере программного комплекса «СёрчИнформ КИБ» [6]) в случае аварийной ситуации в ТР ЦОД. Также приводятся результаты разработки политик и поисковых критериев для DLP-системы, ориентированных на выявление случаев распространения материалов, содержащих призывы к экстремизму и терроризму.

Экстремизм и терроризм как угроза национальной безопасности

Преступления экстремистской и террористической направленности, к сожалению, становятся привычным явлением в жизни общества, состоящего из множества социальных групп, разделяемых между собой как национальной либо расовой принадлежностью, так и религиозными или идеологическими предпочтениями. Противодействие экстремистской и террористической деятельности, связанной с причинением существенного вреда общественным отношениям, обеспечивающим основы конституционного строя, является важнейшим направлением в современной государственной политике противодействия преступности.

В связи с проникновением экстремизма и терроризма в киберпространство их угроза с каждым годом только возрастает. Киберпространство стало интегральной частью современного общества, обеспечивая глобальное взаимодействие, доступ к информации и возможность обмена идеями. Однако, по-

мимо своих позитивных аспектов, оно также предоставляет новые возможности для экстремистских и террористических группировок, которые используют цифровые инструменты в своих интересах [3, 7]. Перед специалистами в области информационной безопасности (ИБ) встает очевидная задача контролировать распространение угроз экстремизма и терроризма в сети и, в случае необходимости, блокировать передачу соответствующей информации при помощи специально разработанных средств (в том числе таких, как DLP-системы).

Использование отечественных средств виртуализации для обеспечения непрерывности функционирования DLP-системы

Ранее отмечалось, что DLP-системы играют ключевую роль в защите конфиденциальной информации. В условиях современной цифровой экономики, когда данные могут располагаться в нескольких ЦОД, важно обеспечить их бесперебойное функционирование, в том числе в случаях аварийных ситуаций и террористических атак. Виртуализация представляет собой эффективное решение для достижения этой цели, предлагая гибкость управления ресурсами и повышенную устойчивость систем. Использование технологий виртуализации для DLP-систем в ЦОД позволяет гарантировать непрерывность сервиса за счет быстрого переноса и восстановления данных на другом сервере внутри ЦОД либо на другом ЦОД, упростить управление и масштабирование за счет реализации централизованного контроля и распределения вычислительных мощностей среди множества виртуальных машин; обеспечить изоляцию и безопасность процессов, что в свою очередь позволяет предотвратить распространение угроз между различными рабочими нагрузками, способствуя устойчивости DLP-системы к внешним и внутренним угрозам; оптимизировать расходы на необходимое оборудование.

Проведенный анализ позволил установить, что оптимальным набором характеристик для виртуализации DLP-систем в ЦОД обладает Программный комплекс «Средства виртуализации «Брест» (ПК СВ «Брест») компании «РусБИТех-Астра» [8]. ПК СВ «Брест» соответствует существующим законодательным требованиям в области ИБ и обеспечивает более высокий уровень защиты от внутренних и внешних рисков по сравнению с иностранными аналогами. Кроме того, применение российских технологий облегчает процесс технической поддержки и обновления программного обеспечения.

В ходе выполненных работ проведен расчет показателей надежности для основных компонент ЦОД, обеспечивающих функционирование DLP-системы: аппаратной части (на примере Huawei FusionServer 2288H V5),

ПК СВ «Брест» и DLP-системы «СёрчИнформ КИБ». Итоговые данные расчета по каждой оцениваемой функциональной подсистеме представлены в табл. 1.

При выходе из строя по причине аварии, терактов или иных экстремистских проявлений одного или нескольких серверов в одном ЦОД с развернутой при помощи ПК СВ «Брест» DLP-системой «СёрчИнформ КИБ» предполагается автоматическая миграция виртуальных машин на резервные или неповрежденные вычислительные мощности внутри того же или другого ЦОД (при наличии связи между ЦОД).

Таблица 1 – Показатели надежности для основных компонент ЦОД, обеспечивающих функционирование DLP-системы.

Параметр	Значение		
	Аппаратная часть	ПК СВ «Брест»	СёрчИнформ КИБ
Интенсивность отказов, 1/ч	0.0001	0.0005	0.0005
Средняя наработка до отказа, ч	10000	2500	2500
Максимальное время восстановления после сбоев, ч	8	8	8
Коэффициент готовности	0.999	0.99	0.99

Разработана методологии восстановления работоспособности DLP-системы, которая включает в себя как немедленные реакции на аварийные ситуации, так и долгосрочные стратегии по восстановлению и оптимизации системы. Методология предусматривает использование модульных подходов и резервирования критически важных компонентов системы. Также предложена процедура регулярных аудитов и тренировок персонала для повышения оперативной готовности к аварийным ситуациям. Проведённые практические испытания методологии на модельных и реальных сценариях аварий в ЦОД позволили оценить её эффективность и выявить потенциальные уязвимости. Результаты испытаний подтвердили значительное сокращение времени восстановления системы и уменьшение потерь данных.

Использование DLP-системы «КИБ СёрчИнформ» в ТР ЦОД

Развертывание DLP-системы «СёрчИнформ КИБ» на облачной платформе дает дополнительные преимущества: бесшовную интеграцию в готовую облачную инфраструктуру с усиленной защитой [9]. Общая схема работы облачной DLP-системы представлена на рис. 1. При этом она обладает полным набором функциональных возможностей: контролирует все каналы передачи информации, качественно анализирует трафик и предоставляет продвинутые

инструменты для расследования инцидентов.

«СёрчИнформ КИБ» позволяет отслеживать: активность в почте (на корпоративном или публичном домене, с доступом через браузер или почтовый клиент); активность в социальных сетях, мессенджерах, телефонии (портативные, десктопные и веб-версии); действия в облачных хранилищах (загрузку, скачивание, удаление и изменение данных); действия с файлами (создание, изменение, удаление файлов на рабочей станции пользователя); действия со съемными устройствами (в том числе подключения к удаленным рабочим столам и виртуальным машинам, использование виртуальных дисков); активность в браузерах (поисковые запросы, посещение сайтов, скачивание и загрузку файлов); активность за ПК (продуктивность и эффективность работы, использование разрешенных/нелегитимных программ и приложений); происходящее на мониторах пользователей (скриншоты и онлайн-просмотр мониторов пользователей, даже если они подключаются к виртуальным средам); другие виды активности пользователей (распечатку документов, аудиопереговоры, действия с клавиатурой, установку/удаление программного обеспечения и т.д.) [10].

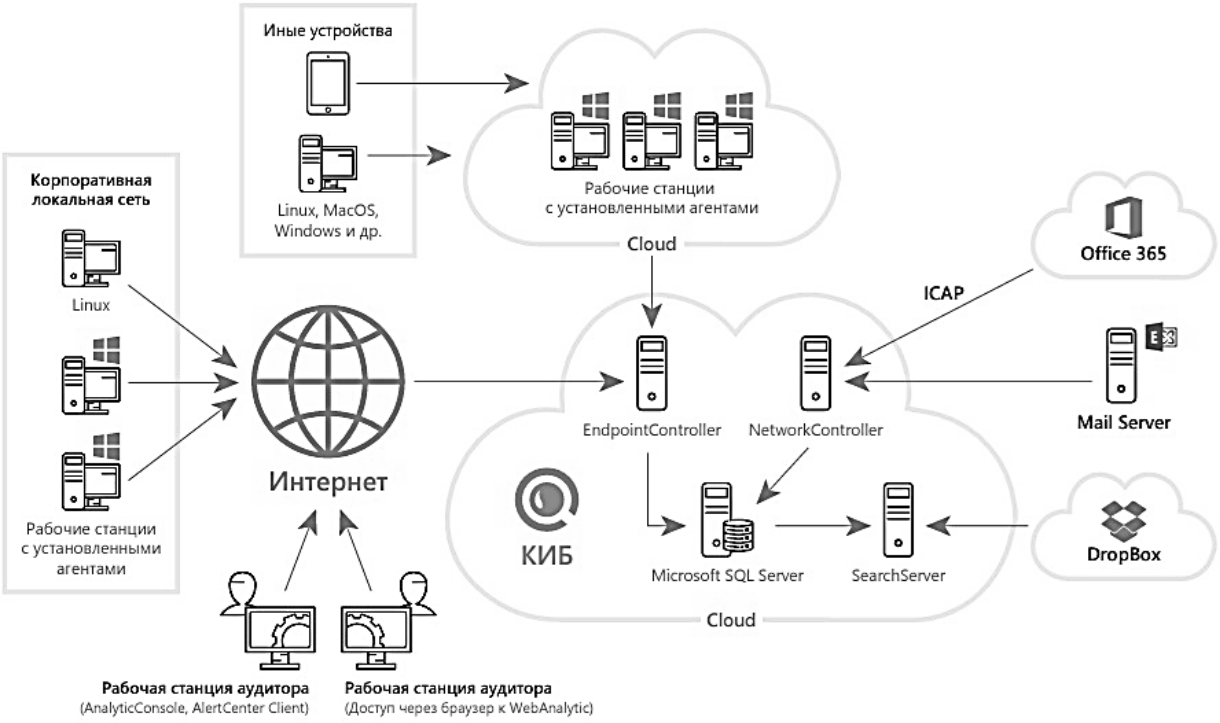

Рисунок 1 – Общая схема работы облачной DLP-системы
на примере «СёрчИнформ КИБ».

В рамках работ по обеспечению непрерывности функционирования DLP-системы «СёрчИнформ КИБ» разработан комплекс критериев и условий поиска, входящих в состав политик безопасности, ориентированных

на предотвращение угрозы распространения экстремизма и терроризма. Для проверки эффективности данных политик создан виртуальный стенд, на котором осуществлялось тестирование и корректировка всех разработанных элементов, и показано, что наилучшего результата позволяет добиться комплексирование поисковых запросов, реализующих фразовый поиск, поиск по словарям и поиск по атрибутам перехваченных сообщений.

Также разработан комплекс технических правил блокировки нежелательных действий пользователей корпоративной сети, связанных с распространением экстремизма и терроризма: контентная блокировка записи на сменные носители информации файлов, имеющих в своем содержании совпадения с данными из списка экстремистских материалов (в том числе с возможностью теневого копирования); блокировка передачи соответствующих материалов при помощи популярных мессенджеров; блокировка посещения сайтов экстремистского характера и отправки на них и др.

Тщательное изучение и анализ механизмов блокировок позволили убедиться в корректности политик и настроек, а также продемонстрировать их эффективность при использовании в корпоративной среде для обеспечения безопасности и грамотного управления ИБ.

Заключение

В работе рассмотрены вопросы обеспечения непрерывности функционирования DLP-системы в случае аварийной ситуации в ТР ЦОД. Установлено, что основные угрозы связаны с рядом технических проблем (например, поломкой оборудования и перебоями в электроснабжении), а также с внешними воздействиями, такими как стихийные бедствия, теракты и целенаправленные кибератаки. Показано, что использование средств виртуализации для поддержания работоспособности DLP-систем в случае аварийных ситуаций в ТР ЦОД не только способствует повышению устойчивости и безопасности ИС, но и обеспечивает их высокую доступность и гибкость управления, что крайне важно для современных организаций в условиях высоких требований к непрерывности и защите данных. На основе результатов анализа разработана методология восстановления работоспособности системы, подтвердившая свою эффективность в ходе практических испытаний. На конкретных примерах обоснована важность политик, используемых для мониторинга распространения материалов, содержащих призывы к экстремизму и терроризму, а также и настроенных правил блокировки, которые играют ключевую роль в обеспечении ИБ и предотвращении возможных инцидентов. Эти политики и правила не только минимизируют риски, но и позволяют специалистам эффективно анализировать полученные

данные, особенно в контексте идентификации и реагирования на террористические и экстремистские угрозы.

Список литературы

1. Осипов А. Автоматизация и ИИ – обязательные элементы современной системы ИБ // Информационная безопасность, 2024. № 2. [Электронный ресурс]. https://www.itsec.ru/ articles/avtomatizaciya-i-ii-obyazatelnye-elementy-sovremennoj-sistemy-ib (Дата обращения: 25.07.24).
2. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Основы управления информационной безопасностью. Серия «Вопросы управление информационной безопасностью. Выпуск 1»: учебное пособие. – М.: Горячая линия-Телеком, 2012. – 244 с.
3. Красинский В.В., Машко В.В. Кибертерроризм: криминологическая характеристика и квалификация // Государство и право, 2023, № 1, с. 79-91.
4. Ли Д. Возможности современных DLP-систем: как защитить внутренние данные компании от утечек [Электронный ресурс]. https://www.anti-malware.ru/analytics/Technology_Analysis/Modern-DLP-systems-capabilities (Дата обращения: 25.07.24).
5. 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.
6. «СёрчИнформ КИБ» [Электронный ресурс]. https://searchinform.ru/products/kib/ (Дата обращения: 25.07.24).
7. Информационная безопасность в системе национальной безопасности [Электронный ресурс]. https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/informatsionnaya-bezopasnost-v-otraslyakh/bezopasnost-informatsionnykh-sistem/informatsionnaya-bezopasnost-v-sisteme-natsionalnoj-bezopasnosti/ (Дата обращения: 25.07.24).
8. ПК СВ «Брест» [Электронный ресурс]. https://astragroup.ru/software-services/application-software-astra-group/brest/ (Дата обращения: 25.07.24).
9. DLP в облаке [Электронный ресурс]. https://searchinform.ru/services/cloud-dlp/ (Дата обращения: 25.07.24).
10. Дрозд А.В., Морозов В.Е, Милославская Н.Г. Основы аналитики в DLP-системах. Программный комплекс «КИБ СёрчИнформ»: учеб.-метод. пособие. – М.: Горячая линия – Телеком, 2023. – 368 с.