DOI 10.37882/2223-2966.2023.11.09

ЗАЩИТА КОНФИДЕНЦИАЛЬНОГО ДОКУМЕНТООБОРОТА НА ОБЪЕКТАХ ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА

PROTECTION OF CONFIDENTIAL DOCUMENT FLOW AT THE FACILITIES OF THE FUEL AND ENERGY COMPLEX

E. Hubert
S. Kozminykh

Summary. Modern information technologies are developing every day and occupy an increasingly important place in the life of society. One of the most important areas of application of information technologies is the fuel and energy complex (fuel and energy complex). Companies working in the fuel and energy sector process a large amount of confidential information, including through electronic document management (EDI). The use of EDI allows you to speed up the processes of information exchange, reduce the cost of paper documentation and reduce the time for the execution of contracts. However, the use of EDI is also associated with threats to information security, which can lead to serious consequences for the company and its customers. This article discusses the classification of electronic document management systems and the possibilities of the most popular of them. The issues of information security are also analyzed based on the functionality of the presented electronic document management systems.

Keywords: electronic document management, EDMS, information threats, data protection.

Губерт Екатерина Сергеевна
Аспирант, Финансовый университет при Правительстве Российской Федерации
katia42rus@mail.ru
Козьминых Сергей Игоревич
Доктор технических наук, профессор, Финансовый университет при Правительстве Российской Федерации

Аннотация. Современные информационные технологии развиваются с каждым днем и занимают все более важное место в жизни общества. Одной из самых важных сфер применения информационных технологий является топливно-энергетический комплекс (ТЭК). Компании, работающие в сфере ТЭК, обрабатывают большое количество конфиденциальной информации, в том числе через электронный документооборот (ЭДО). Использование ЭДО позволяет ускорить процессы обмена информацией, уменьшить затраты на бумажную документацию и сократить время исполнения договоров. Однако использование ЭДО также связано с угрозами информационной безопасности, которые могут привести к серьезным последствиям для компании и ее клиентов. В данной статье рассматривается классификация систем электронного документооборота и возможности наиболее популярных из них. Также анализируются вопросы информационной безопасности исходя из функциональности представленных систем электронного документооборота.

Ключевые слова: электронный документооборот, СЭД, угрозы информации, защита данных.

Функционирование современного предприятия невозможно без эффективной системы документооборота. Традиционные методы обработки документов, такие как бумажные документы и обычные электронные письма, уже не могут удовлетворять все более высокие потребности в быстроте, надежности и безопасности. В этой связи, электронный документооборот (ЭДО) становится необходимым инструментом для обслуживания бизнес-процессов на производствах и предприятиях, в том числе и на топливно-энергетических комплексах.

Первые упоминания об ЭДО появились в 1960-х годах, когда компьютеры стали использоваться в коммерческих целях. Однако, первый полноценный пример электронного документооборота был реализован только в 1970 году в рамках проекта EDI (Electronic Data Interchange), который был разработан для автоматизации процессов бизнес-коммуникации между компаниями. В настоящее время электронный документооборот широко используется во многих отраслях экономики и является неотъемлемой частью современных технологий управления документами и бизнес-процессами.

Система ЭДО должна улучшить рабочие процессы за счет определенных функций автоматизации и возможности легко оцифровывать бумажные документы. Четко классифицировать системы электронного документооборота (СЭД) достаточно проблематично, в связи с тем, что один ее вид может содержать несколько элементов или признаков другого, но, в принципе, каждая СЭД ориентирована вполне конкретно.

Электронные архивы (ЭА) — это хранилища электронных документов, все их возможности ориентированы на хранение больших объемов данных и быстрый поиск нужной информации.

СЭД с развитыми workflow-средствами (WF) — довольно сложны в организации и предполагают жесткую маршрутизацию с привязкой документов к соответствующим операциям. Данные СЭД содержат функциональность, позволяющую создавать сложные бизнес-процессы, задавать шаблоны документов, автоматически регламентировать сроки выполнения задач, контролировать выполнение работниками различных отделов и формировать аналитические отчеты.

Системы типа коллабораций (collaboration) — это информационные системы, основанные на принципах совместной работы и сотрудничества, которые обеспечивают хранение, обмен и управление документами между участниками процесса. Они позволяют автоматизировать процессы документооборота, ускорить их выполнение и повысить эффективность работы команды, участники которой работают удаленно или находятся в разных местах. Данные СЭД также обеспечивают контроль за доступом к документам и аудит действий, связанных с их обработкой и хранением.

СЭД с опциями CRM — кроме организации работы с документами, содержат данные для взаимодействия с клиентами и партнерами.

ECM-системы (Enterprise Content Management) — это комплексный подход к управлению информационными ресурсами организации, направленный на улучшение процессов сбора, хранения, обработки и распространения электронных документов и других корпоративных данных. ECM-системы включают в себя различные технологии и методы, такие как документооборот, электронное хранилище, управление версиями, автоматизация бизнес-процессов, поиск и фильтрацию информации, средства аналитики и отчетности, а также соответствующие политики безопасности и защиты данных.

По данным исследования TAdviser [4] рынок систем электронного документооборота в России показал уверенный рост в 2022 году. Благодаря государственной поддержке и курсу на импортозамещение существующих зарубежных платформ, объем российского рынка СЭД и ECM, прогнозируемого на 2023 год, выше на 10 % по сравнению с 2022 годом и составляет 77,7 млрд рублей. Это обусловлено тем, что эффективность ЭДО признана практически повсеместно, СЭД позволяет упростить и оптимизировать процесс создания, согласования, сортировки и хранения документов любого уровня, снизить количество служб и время отдельных этапов работы.

Отсутствие потребности вручную размножать документы, отслеживать передвижение бумажных документов внутри компании, осуществлять контроль процедуры передачи конфиденциальных данных необходимым способом уменьшает трудовые затраты делопроизводителей. Сквозной автоматизированный контроль исполнения во всех этапах работы с документами существенно увеличивает качество деятельности исполнителей, делает сроки подготовки документов наиболее прогнозируемыми и контролируемыми. Одновременное использование систем электронного делопроизводства и хранилищ информации может помочь систематизировать и группировать информацию, что точно сделает её анализ и формирование отчётов существенно легче (рис. 1) [1].

Наиболее же популярными системами документооборота в стране, согласно обзору от компании Comindware [2] являются пять платформ, предоставляющих бизнесу более широкий спектр возможностей: Directum, 1С:Документооборот, Дело, Тезис, DocVision. В таблице 1 отображено сравнение специальных опций и функционала, присущих каждой из представленных систем ЭДО, которые отразились бы на безопасности хранимой в них информации.

Но пользователей часто волнует не только вопрос удобства работы с программой, актуальной становится задача сохранения важной информации при работе с договорами или конфиденциальной перепиской.

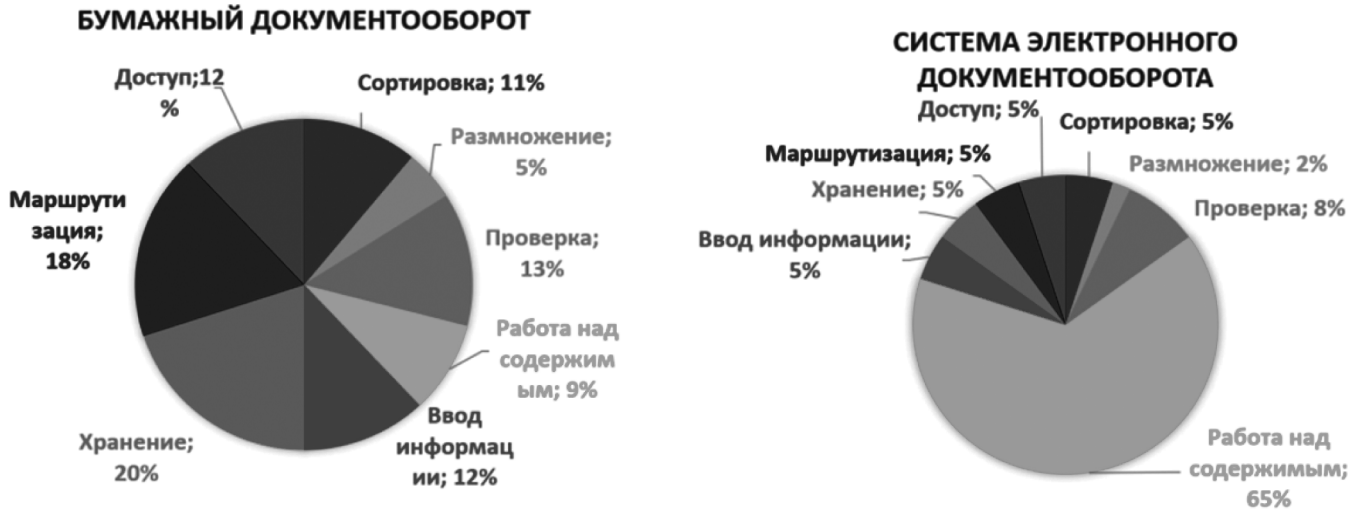

Рис. 1. Сравнение времени, затраченного на отдельные этапы работы с документами при замене бумажного процесса на цифровой

Таблица 1.

Сравнение решений

Функции	Directum	1С: Документооборот	Дело	Тезис	DocVision
Установка на свой сервер	+	+	+	+	+
Web-клиент	+	–	+	+	+
Возможность назначения ответственного исполнителя по документу	–	–	+	+	-
Создание документа по шаблону	+	+	+	+	+
Рассылка уведомлений по электронной почте	+	+	+	+	+

1. Угрозы информационной безопасности конфиденциального ЭДО на объектах ТЭК

Компании, работающие в сфере ТЭК, обрабатывают большое количество конфиденциальной информации, например, такой как:

— коммерческие и технические соглашения с партнерами и клиентами;
— планы и отчеты по производственной деятельности;
— данные о финансовых и кадровых ресурсах компании;
— информация о защите окружающей среды в районах добычи, транспортировки и хранения ресурсов;
— технические характеристики оборудования и технологические решения;
— интеллектуальная собственность и технические изобретения, применяемые при разработке и производстве;
— информация о закупках и их выполнении, и т.д.

Конфиденциальный электронный документооборот на объектах ТЭК позволяет ускорить процессы обмена информацией, уменьшить затраты на бумажную документацию и сократить время исполнения договоров. Однако использование ЭДО представляет собой огромную угрозу для безопасности сектора энергетики.

Последствия утечки информации на объектах топливно-энергетического комплекса могут быть катастрофическими и даже привести к гибели людей. Кроме того, утечка может привести к серьезным экологическим последствиям, загрязнению водных ресурсов и почвы, а также нанести ущерб экономике. Возможными последствиями являются аварии и взрывы, выход вредных веществ в атмосферу, загрязнение грунтовых вод и поверхностных водоемов, нарушение экосистемы, угроза здоровью людей и животных.

Угрозы для систем ЭДО достаточно стандартны. Угроза целостности, конфиденциальности и работоспособности системы. Защиту именно от этих угроз в той или иной мере должна реализовывать любая система ЭДО.

В таблице 2 представлен анализ угроз информационной безопасности, определена вероятность их наступления и возможные последствия причиненного ущерба.

Оказывается, конфиденциальный электронный документооборот на объектах ТЭК подвержен множеству угроз информационной безопасности. Рассмотрим модель угрозы утечки информации, состоящую из четырех параметров:

— вероятность возникновения угрозы (P)
— вероятность обнаружения угрозы (D)
— уровень уязвимости информации (V)
— уровень защиты информации (Z)

Тогда математическая модель угрозы утечки информации может быть представлена следующим образом:

$$I = P * V * (1 — D) / Z \quad (1)$$

где I — интенсивность утечки информации.

Параметр P определяет вероятность возникновения угрозы, которая может быть оценена на основе анализа исторических данных и экспертных оценок.

Параметр D отражает вероятность обнаружения угрозы, которая может быть определена на основе систем мониторинга и защиты информации.

Параметр V определяет уровень уязвимости информации, который может быть оценен на основе анализа уязвимостей системы и данных.

Параметр Z отражает уровень защиты информации, который может быть определен на основе использования соответствующих мер защиты информации.

Математическая модель угрозы утечки информации позволяет оценить риски возникновения угрозы и принять меры по уменьшению этих рисков, вместе с тем, модель киберпреступника позволит оценить вероятность совершения преступления и определить меры по предотвращению кибератак.

Киберпреступники активно действуют, используя различные методы атак, чтобы получить доступ к конфи-

Таблица 2.

Перечень угроз конфиденциального ЭДО на объектах ТЭК

№	Угрозы системы ЭДО	Вероятность наступления угрозы	Последствия осуществления угрозы
1.	Утечка конфиденциальной информации	Высокая	Раскрытие конфиденциальных данных, утечка информации о бизнес-процессах, финансовых операциях и т.д.
2.	Вирусная атака	Высокая	Повреждение файлов, нарушение работы системы, потеря данных
3.	Фишинг	Средняя	Получение злоумышленниками доступа к конфиденциальной информации, утечка информации о бизнес-процессах, финансовых операциях и т.д.
4.	DDoS-атака	Средняя	Перегрузка серверов, недоступность системы, потеря данных
5.	Несанкционированный доступ	Высокая	Утечка информации, потеря данных, нарушение работоспособности системы
6.	Социальная инженерия	Средняя	Получение злоумышленниками доступа к конфиденциальной информации
7.	Рассылка спама	Высокая	Потеря времени на фильтрацию нежелательных сообщений
8.	Угрозы, связанные с использованием мобильных устройств	Средняя	Утечка информации, потеря данных, нарушение работоспособности системы
9.	Вредоносное программное обеспечение	Высокая	Повреждение файлов, нарушение работы системы, потеря данных
10.	Кибершпионаж	Средняя	Утечка конфиденциальной информации
11.	Угроза физической безопасности	Средняя	Нарушение работоспособности системы, потеря данных
12.	Нарушение доступности системы	Высокая	Недоступность системы, потеря данных
13.	Угрозы, связанные с облачными технологиями	Средняя	Утечка информации, потеря данных, нарушение работоспособности системы
14.	Внутренние угрозы	Высокая	Утечка конфиденциальной информации, потеря данных

денциальным данным. Они используют все возможные уязвимости в структуре данных, чтобы быстро и эффективно получить необходимую информацию. Это может быть уязвимость в программном обеспечении, слабый пароль, проблемы с защитой персональных данных и многое другое.

Математическая модель киберпреступника может быть представлена следующим образом:

Киберпреступник = (Навыки + Мотивация + + Возможности) * Среда

где:

- — Навыки — уровень технических знаний и навыков, необходимых для совершения киберпреступлений;
- — Мотивация — причины, побуждающие киберпреступника к совершению преступлений (например, финансовая выгода, политические мотивы, желание навредить другим);
- — Возможности — наличие доступа к необходимым инструментам и ресурсам для совершения киберпреступлений (например, уязвимости в системах, слабые пароли, доступ к конфиденциальной информации);
- — Среда — общественно-экономические, политические и технологические условия, в которых действует киберпреступник (например, уровень защиты информационных систем, наличие законодательства, политическая стабильность).

Основываясь на функциональных возможностях, отраженных в таблице 1, проанализируем актуальные риски нанесения ущерба от потери конфиденциальной информации (утечки данных) при использовании систем ЭДО на объектах ТЭК.

В качестве первого функционального решения указана функция «установка на свой сервер», и все рассматриваемые системы ЭДО предлагают данную опцию. Серверы играют ключевую роль в обработке и хранении конфиденциальных для бизнеса данных. Защита серверов от внешних угроз с помощью мер безопасности сервера имеет важное значение для обеспечения безопасности конфиденциальной информации. В качестве распространенных типов угроз для сервера выделяют DDoS атаки, атаки методом перебора и неосторожные или злонамеренные действия пользователей.

Вторая опция, в сравнительной таблице, которая не поддерживается только у современной СЭД 1С:Документооборот — это «Web-клиент». Стандартные функции Web-клиентов обеспечивают возможность использования WWW как интегрирующего сервиса. Современная веб-архитектура в значительной степени

зависит от JavaScript и позволяет стороннему коду выполнять сетевые запросы на стороне клиента. К типовому классу кибератак в области web-клиентов выделяют проблемы на уровне инфраструктуры хостинга и угрозы в области сетевой безопасности. Это и XSS (межсайтовый скриптинг), и инъекции контента, и атаки типа Man In The Browser.

Функция, осуществляемая возможность назначения ответственного исполнителя по документу присутствует только в двух рассматриваемых решениях ЭДО. Данная функция очень важна при организационных мерах безопасности при работе с конфиденциальными данными. Согласно отчету компании Verizon о расследовании нарушений данных за 2022 год «человеческий фактор» продолжает оставаться доминирующей тенденцией [3]. Назначение ответственного исполнителя в ЭДО позволит сотруднику более осмысленно выполнять действия по работе с конфиденциальными данными и предотвратить несанкционированное уничтожение документов с важной информацией, передачу ложных сведений и разглашение служебных тайн. Внутреннее расследование моментально определит, кто из сотрудников виновен в той или иной утечке.

Отсутствие шаблонов и стандартов типовых документов увеличивает временные затраты на обработку, поддержку единого стиля документации, отсюда актуализируются все типовые риски, связанные с конфиденциальностью, содержанием и оформлением документов. Типовые документы уже учитывают все необходимые требования и критерии, важные для бизнеса (например, требования compliance, или соображения информационной безопасности и т.п.). Ведь унификация документов экономит массу ресурсов для их создания, обсуждения, разносторонней экспертизы.

Процесс рассылки уведомлений по электронной почте также позволяет минимизировать риски утечек данных при работе в системах конфиденциального ЭДО. Система уведомлений позволяет уведомлять администраторов ЭДО об оповещениях, нарушениях политики безопасности и изменениях статуса выполняемых задач. Благодаря оповещениям от системы ЭДО пользователи смогут проследить все этапы жизненного цикла документа, а соответствующий ИТ-персонал своевременно отреагировать и разрешить возможные проблемы, связанные с безопасностью.

Модель незаконного воздействия на защищаемый документооборот может включать следующие шаги:

1. Определение уязвимостей в системе защиты документооборота, например, недостаточной шифровки данных, отсутствия многофакторной аутентификации и т.д.
2. Перехват данных, передаваемых по защищенному каналу связи, например, за счет использования вредоносных программ или анализа трафика сети.
3. Изменение, подмена или уничтожение передаваемых данных, например, внедрением вредоносного кода в документ или изменением его содержания в процессе передачи.
4. Получение несанкционированного доступа к хранилищу документов, например, путем взлома системы аутентификации или использования слабых паролей.
5. Утечка конфиденциальной информации, например, за счет несанкционированного доступа к документам или их копирования.
6. Нанесение ущерба бизнесу, например, путем блокировки доступа к документам или их изменения.
7. Сокрытие преступного следа, например, путем удаления журналов аудита или изменения метаданных документов.

Таким образом, конфиденциальный электронный документооборот на объектах ТЭК подвержен множеству угроз информационной безопасности.

2. Методы и средства защиты от угроз информационной безопасности конфиденциального ЭДО на объектах ТЭК

Итак, было выяснено, что конфиденциальные данные, передаваемые по сетям связи, могут быть скомпрометированы злоумышленниками. В связи с этим, важно разработать и применять эффективные методы и средства защиты от угроз информационной безопасности конфиденциального ЭДО на объектах ТЭК. И первоочередная задача — это внедрение организационных мер, которые соответствуют требованиям законодательства и запретным нормам, а также адаптированы к конкретным условиям работы объектов ТЭК. К данным мерам можно отнести:

1. Разработка и утверждение политики безопасности. В данной политике должны содержаться определенные правила, процедуры и рекомендации по обеспечению безопасности конфиденциального документооборота и использованию технических средств защиты.
2. Создание централизованной системы управления доступом к электронным документам — это позволит контролировать доступ к информации в зависимости от роли и прав пользователей.
3. Установка системы мониторинга доступа к электронным документам — это обеспечит контроль за действиями пользователей, а также поможет выявить несанкционированные попытки доступа к конфиденциальной информации.
4. Регулярное проведение обучения сотрудников — обучение сотрудников правилам работы с электронными документами и обеспечению

безопасности является важным мероприятием для снижения риска возникновения внутренних угроз.

5. Разработка и внедрение процедуры контроля безопасности на объектах ТЭК — это меры, направленные на устранение уязвимостей в системе обработки электронных документов через проверку программного обеспечения и оборудования, подключенного к сети.
6. Регулярное обновление и обслуживание технических средств защиты информации — это поможет удержать уровень безопасности на необходимом уровне и снизить радиус уязвимости системы.

По результатам анализа перечисленных мер защиты от угроз информационной безопасности конфиденциального ЭДО на объектах ТЭК сделан вывод о целесообразности внедрения программных средств защиты информации.

В качестве таких программных продуктов можно предложить комплексные решения, используемые в сфере информационной безопасности для защиты конфиденциальной информации. Такие решения позволяют определить, контролировать и защищать данные в режиме реального времени, предотвращая несанкционированный доступ к ним, утечку и уничтожение. Такие решения определяют уязвимости в защите данных и предоставляют рекомендации по усовершенствованию мер безопасности.

Пример общей схемы работы системы для защиты конфиденциальной информации представлен на рисунке 2.

1) SIEM (Security Information and Event Management) — это инструмент для обнаружения и реагирования на угрозы информационной безопасности в режиме реального времени. SIEM обеспечивает централизованный сбор, агрегирование и анализ массивов данных в масштабах всего предприятияй и позволяет эффективно оптимизировать рабочие процессы, связанные с безопасностью.

SIEM система может помочь предприятиям ТЭК в следующих областях:

1. Обнаружение и предотвращение кибератак: SIEM система позволяет мониторить события, происходящие на сетевых устройствах и серверах, а также анализировать данные журналов безопасности

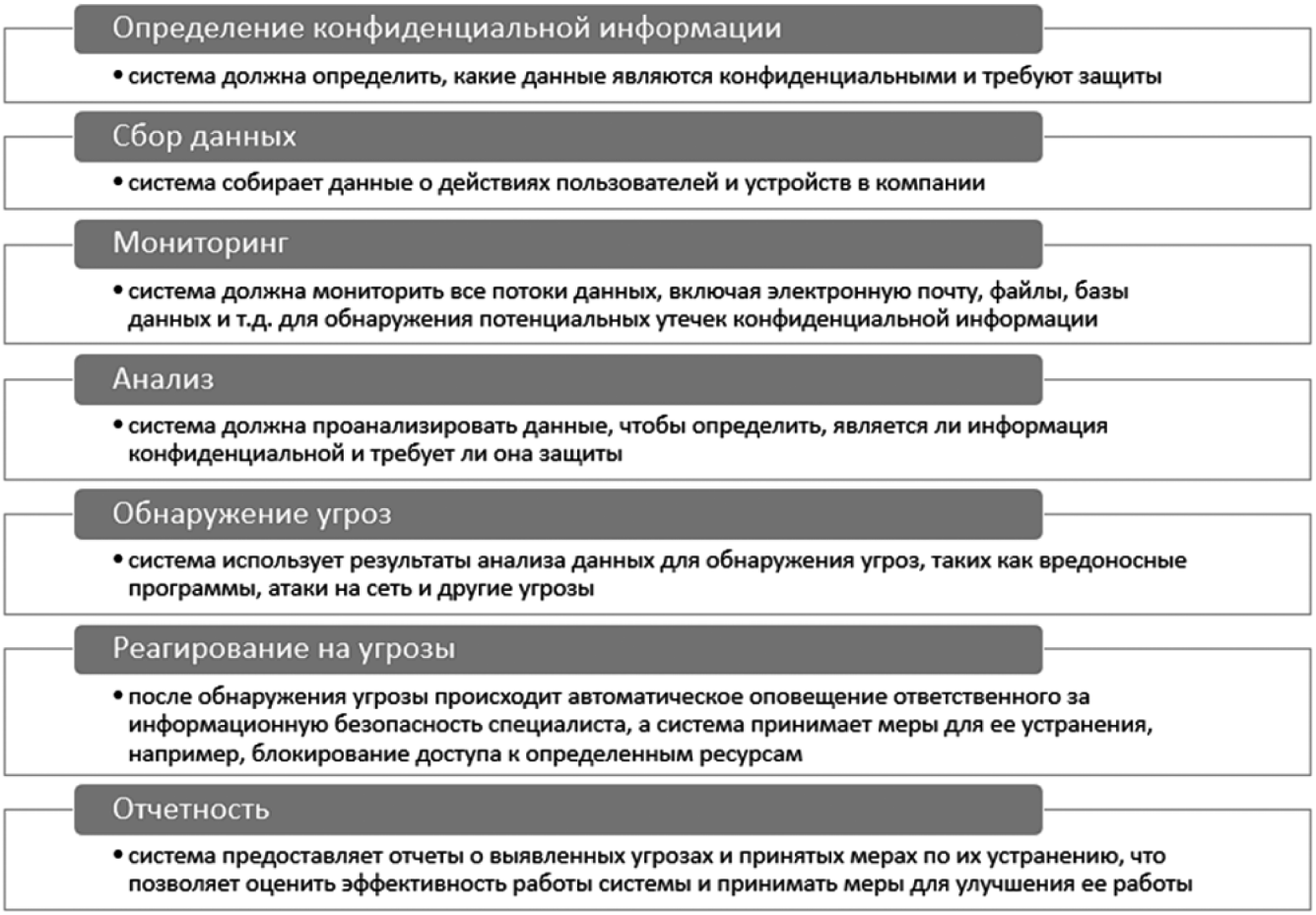

Рис. 2. Схема работы программных решений в области безопасности

для выявления потенциальных угроз. Это позволяет оперативно реагировать на инциденты и принимать меры по защите от кибератак.
2. Управление доступом: SIEM система может использоваться для контроля доступа пользователей к различным ресурсам компании, например, базам данных или приложениям. Систему можно настроить таким образом, чтобы она автоматически блокировала доступ пользователя в случаях несанкционированного использования.
3. Мониторинг соответствия стандартам безопасности: SIEM систему можно использовать для проверки соответствия компании требованиям закона или стандартам безопасности (например, PCI DSS). Системой можно проводить аудит информационной инфраструктуры предприятий ТЭК и выдавать отчеты о технических недостатках.
4. Аудит действий пользователей: SIEM система позволяет отслеживать действия пользователей в информационной инфраструктуре предприятий ТЭК. Это помогает выявлять нарушения безопасности, связанные с неправомерным использованием ресурсов компании.
5. Улучшение производительности и оптимизация ресурсов: SIEM система может быть использована для мониторинга производительности серверов и сетевых устройств, а также для определения проблем в работе приложений или баз данных. Это может помочь предприятию ТЭК оптимизировать использование ресурсов и улучшить производительность системы в целом.

2) UEBA (User and Entity Behavior Analytics) — это инструмент для обнаружения аномального поведения пользователей и устройств в компании, позволяет компаниям быстро реагировать на необычное поведение пользователей и предотвращать потенциальные проблемы в области информационной безопасности, связанные с человеческим фактором (например, кража данных, утечка конфиденциальной информации и т.д.).

UEBA система может помочь предприятиям ТЭК в следующих областях:
1. Обнаружение угроз безопасности: UEBA система анализирует поведение пользователей и сущностей на предприятии, чтобы выделить необычные или подозрительные действия. Это позволяет быстро обнаруживать потенциальные угрозы безопасности, такие как кража данных или злоупотребление привилегиями.
2. Управление доступом: UEBA система может помочь определить правильный уровень доступа для каждого пользователя и сущности на основе его поведения и роли в организации. Это позволяет минимизировать риски, связанные с неправильным использованием привилегий.
3. Отслеживание изменений конфигурации: UEBA системы могут отслеживать изменения конфигурации приложений, баз данных и других инфраструктурных компонентов для быстрого выявления возможных ошибок или аномалий.
4. Мониторинг активности поставщиков услуг: в случаях, когда компания использует услуги сторонних поставщиков IT-услуг (например хостинг), то можно использовать UEBA-систему для мониторинга их активности, чтобы убедиться в том, что они не нарушают политики безопасности предприятия.
5. Улучшение производительности: UEBA системы могут помочь оптимизировать рабочие процессы и повысить эффективность работы сотрудников путем анализа данных об использовании приложений и других инструментов.
6. Соблюдение нормативных требований: UEBA системы помогают компаниям ТЭК соблюдать нормативные требования, такие как GDPR (Общий регламент по защите данных). UEBA системы позволяют автоматически отслеживать нарушения политик безопасности и предупреждать о возможных проблемах до того, как они станут серьезными. Кроме того, UEBA системы могут помочь компании быстро реагировать на запросы соответствующих контролирующих органов или аудиторских проверок.

3) EDR (Endpoint Detection and Response) система — это инструмент, который используется для обнаружения и реагирования на угрозы, которые могут возникнуть на конечных устройствах в сети.

EDR система может помочь предприятиям ТЭК в следующих областях:
1. Обнаружение и предотвращение кибератак: EDR система позволяет быстро обнаруживать аномальную активность на конечных устройствах, таких как компьютеры и мобильные устройства, что позволяет оперативно реагировать на потенциальные киберугрозы.
2. Мониторинг безопасности сети: EDR система способна отслеживать все подключенные к сети устройства и контролировать доступ пользователей, что повышает безопасность всей инфраструктуры.
3. Аудит действий пользователей: Система EDR фиксирует все действия пользователя на конечном устройстве, что позволяет выявлять некомплектное использование корпоративной информации или злоупотребление правами доступа.
4. Управление рисками: благодаря возможности быстрого определения причин возникновения проблем в работе IT-систем можно своевременно провести необходимые мероприятий по миними-

зации рисков для бизнес-достижений компаний ТЭК.
5. Повышение эффективности работы ИТ-специалистов: EDR система позволяет автоматизировать процессы мониторинга и анализа данных, что упрощает работу ИТ-специалистов и повышает эффективность работы всей команды.

4) NAC (Network Access Control) система — это инструмент, который используется для контроля доступа к сети.

NAC система может помочь предприятиям ТЭК в следующих областях:
1. Безопасность сети: NAC система позволяет контролировать доступ к сети и управлять правами пользователей на основе политик безопасности, что повышает защиту от внешних и внутренних угроз.
2. Управление рисками: NAC система позволяет автоматически определять несанкционированные устройства, которые могут быть потенциальной точкой проникновения для злоумышленников или программного обеспечения-вредоносных программ.
3. Соблюдение нормативных требований: NAC система помогает предприятию ТЭК соответствовать различным нормам и стандартам безопасности данных, таким как PCI DSS или HIPAA.
4. Улучшение производительности сети: благодаря контролю доступа к сетевым ресурсам на основе политик безопасности, можно избежать перегрузок и конфликтов при использовании широкого спектра приложений.
5. Централизация администрирования: NAC система позволяют централизованно управлять всеми устройствами, подключенными к сети предприятия ТЭК. Это облегчает задачу администраторов и повышает эффективность работы всей команды.

5) IAM (Identity and Access Management) система — это инструмент, который используется для управления и контроля доступа к ресурсам и приложениям в организации.

IAM система может помочь предприятиям ТЭК в следующих областях:
1. Управление доступом: IAM система позволяет управлять доступом к различным ресурсам и приложениям на предприятии, таким как базы данных, серверы, электронная почта и т.д. Это помогает защитить конфиденциальную информацию от несанкционированного доступа.
2. Автоматизация процессов: IAM система может автоматизировать процессы создания новых пользователей или изменения прав доступа существующих пользователей на основе определенных правил и политик безопасности.
3. Уменьшение затрат: IAM системы могут снизить затраты на администрирование учетных записей пользователями благодаря автоматизации процессов создания/удаления аккаунтов.
4. Обеспечение соответствия требованиям законодательства: IAM системы могут помочь предприятию ТЭК быть в соответствии с требованиями закона о защите персональных данных или другими нормами безопасности информации.
5. Предупреждение утечек данных: Использование IAM системы может помочь предотвратить утечки данных, так как она позволяет контролировать доступ к конфиденциальной информации и отслеживать действия пользователей.
6. Улучшение производительности: IAM система может улучшить производительность сотрудников, обеспечивая им быстрый и безопасный доступ к необходимой информации.

В целом, IAM система является важным инструментом для предприятий ТЭК, которые стремятся обеспечить безопасность своих данных и повысить эффективность работы сотрудников.

6) DLP (Data Loss Prevention) система — это комплексные решения, используемые в сфере информационной безопасности для защиты конфиденциальной информации.

DLP система может помочь на объектах ТЭК в следующих сценариях:
1. Мониторинг и контроль за передачей конфиденциальной информации через электронную почту, мессенджеры, облачные хранилища и другие каналы связи.
2. Ограничение доступа к конфиденциальной информации только для авторизованных пользователей.
3. Обнаружение и блокирование попыток несанкционированного доступа к конфиденциальной информации.
4. Мониторинг и контроль за использованием съемных носителей, таких как USB-накопители, CD/DVD-диски и т.д.
5. Анализ и классификация конфиденциальной информации, что позволяет определить, какие данные являются наиболее ценными и требуют наибольшей защиты.

7) CASB (Cloud Access Security Broker) система — это инструмент, который используется для обеспечения безопасности при работе с облачными сервисами.

Основные этапы работы CASB системы включают в себя:
1. Обнаружение облачных сервисов: CASB система сканирует сеть и обнаруживает все облачные сервисы, которые используются в организации.

2. Классификация данных: CASB система классифицирует данные, которые передаются через облачные сервисы, на основе их конфиденциальности и чувствительности.
3. Мониторинг активности: CASB система мониторит активность пользователей в облачных сервисах, чтобы обнаружить любые подозрительные действия.
4. Контроль доступа: CASB система контролирует доступ к облачным сервисам, используя политики безопасности, которые определяют, кто может получить доступ к каким данным.
5. Защита данных: CASB система защищает данные, которые передаются через облачные сервисы, используя шифрование и другие методы защиты.
6. Аудит и отчетность: CASB система предоставляет аудит и отчетность о действиях пользователей в облачных сервисах, чтобы обеспечить соответствие требованиям безопасности и законодательства.

Соответственно, CASB система на предприятиях ТЭК может помочь в защите данных, которые хранятся и обрабатываются в облачных сервисах. Она позволяет контролировать доступ к облачным приложениям и сервисам, а также мониторить и анализировать трафик данных, проходящий через них. CASB система может обнаруживать и предотвращать утечки данных, а также защищать от вредоносных атак и несанкционированного доступа к облачным ресурсам.

Таким образом, указанные выше системы являются мощными средствами обеспечения безопасности информационной инфраструктуры предприятий ТЭК. Такие инструменты позволяют оперативно выявлять потенциальные угрозы, контролировать доступ пользователей к ресурсам компании и проводить аудит действий пользователей. Кроме того, подобные системы могут быть применены для оптимизации использования ресурсов и повышения производительности информационной инфраструктуры на объектах ТЭК.

Заключение

Системы ЭДО помогают оптимизировать ключевые процессы предприятия, сократить затраты и время на обработку документов, повысить ответственность сотрудников. Работа без ЭДО сегодня — это потеря времени и возможных клиентов бизнеса. Все хотят работать быстро, без бумажной волокиты, потерянных договоров и ошибок. А время и средства на распечатку, хранение, поддержание порядка в архивах и физическую пересылку можно направить на решение других бизнес-задач, но не стоит забывать про безопасность, которую должна обеспечивать система ЭДО.

У разных систем ЭДО есть свои сильные и слабые стороны защиты конфиденциальных документов. При выборе систем ЭДО необходимо отталкиваться не только от своих основных задач, масштабов организации, и финансовых возможностей, но и обращать внимание на уровень безопасности, предлагаемый разработчиками систем ЭДО.

Для использования конфиденциального электронного документооборота на объектах ТЭК с учетом угроз информационной и технической безопасности следует руководствоваться следующими рекомендациями:

1. Определить уровень защищенности информации, необходимый для объектов ТЭК.
2. Выбрать специальные программные решения, обеспечивающие конфиденциальность документов и защиту от утечек информации.
3. Обеспечить систему аутентификации пользователей, использующих электронный документооборот.
4. Использовать специальные средства шифрования данных при передаче и хранении документов.
5. Установить систему мониторинга, позволяющую отследить доступ к конфиденциальным документам и выявить возможные нарушения безопасности.
6. Обучить сотрудников, работающих с электронными документами, правилам обращения с конфиденциальной информацией и мерам безопасности.
7. Проводить регулярные аудиты и проверки системы электронного документооборота на предмет обнаружения уязвимостей и нарушений безопасности.

Необходимое действие для защиты конфиденциальных данных на объектах ТЭК — это использование программных решений в сфере информационной безопасности, ведь одним из главных преимуществ представленных систем является возможность предотвращения потенциальных угроз.

ЛИТЕРАТУРА

1. DBIR Report 2022 — Summary of Findings | Verizon Business [Электронный ресурс]. — Режим доступа: https://www.verizon.com/business/en-sg/resources/reports/dbir/2022/summary-of-findings.
2. TAdviser: Новости ИТ-рынка России [Электронный ресурс]. — Режим доступа: https://www.tadviser.ru/index.php/СЭД.
3. Алисевич Е.А., Бухарин В.В., Гречишников Е.В., Милая И.В., Панкова Н.В., Стародубцев Г.Ю., Стародубцев Ю.И. Способ обеспечения защищенности автоматизированных систем // Патент России № 2477881 28.11. 2011.Бюл. № 8
4. В.А. Волостных, П.А. Кононов, А.В. Петров «Организация электронного документооборота в учреждении» — СПб.: Сборник научных статей VIII «Международной научно-технической конференции АПИНО-2019».
5. Валявина, К.М. Совершенствование документооборота организации в современном мире / К.М. Валявина. — Текст: непосредственный // Вестник Уральского института экономики, управления и права. — 2020. — № 4. — С. 82–85.
6. Данилова Е.И., Лаута О.С., Ракицкий Д.С., Ракицкий С.Н. Подход к построению модели целевых кибернетических воздействий // В сборнике: Актуальные проблемы защиты и безопасности Труды XXII Всероссийской научно-практической конференции РАРАН. 2019. С. 210–213.
7. Игнатенко К.А., Левин Ю.В., Мартынюк И.А., Штаненко В.И. Технические каналы утечки конфиденциальной информации. // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018) VII Международная научно-техническая и научно методическая конференция. Сборник научных статей. В 4-х томах. Под редакцией С.В. Бачевского. 2018. С.414–418
8. Калугина, Е.А. Система электронного документооборота, ее преимущества и переход на электронный документооборот / Е.А. Калугина. — Текст: непосредственный // Вестник Национального института бизнеса. — 2019. — № 40. — С. 110–113.
9. Киселев, А.А. Разработка комплексной защиты электронного документооборота предприятия: Автореф. дис. кан. техн. наук. — М.: 2006. — 27 с.
10. Концепция построения автоматизированной информационной системы Министерства обороны Российской Федерации: утверждена министром обороны Российской Федерации. Москва. 2008. 9 с.
11. Липатников В.А., Тихонов В.А., Шевченко А.А. Метод управления кибернетической безопасностью в системах критических инфраструктур, основывающийся на интеллектуальных сервисах защиты информации. В сборнике: Технологии построения когнитивных транспортных систем. Материалы всероссийской научно-практической конференции с международным участием. 2019. — С. 207–214.
12. Национальный открытый университет «Интуит» [Электронный ресурс]. — Режим доступа: https://intuit.ru/studies/courses/76/76/lecture/27928?page=2.
13. Стародубцев Ю.И. Экономика цифровых информационных услуг: монография/ Ю.И. Стародубцев, М.А. Давлятова; под общей редакцией заслуженного деятеля науки РФ профессора Ю.И. Стародубцева. — СПб.: ПОЛИТЕХ-ПРЕСС, 2019. — 452 с.
14. Стародубцев Ю.И., Сухорукова Е.В., Чукариков А.Г. Методика выявления критически важных элементов информационно-телекоммуникационных систем // Проблемы 23 экономики и управления в торговле и промышленности. 2014. № 1 (5). С. 95–101.
15. Сухаревская Е.В., Михальченко С.В., Шамин И.М., Никишова А.В. Методы защиты доступа в ERP-системах: идентификация и аутентификация // Молодой ученый. — 2016. — №20. — С. 205–207. — Режим доступа: https://moluch.ru/archive/124/34215/
16. Тесля С.П., Мартынюк И.А., Федоров С.В., Чоп А.А. Подход к обоснованию требований к средствам защиты информационно-телекоммуникационной сети. // В сборнике: Региональная информатика и информационная безопасность 2017. С. 172–173.
17. Топ 10 СЭД-систем для электронного документооборота 2023 года [Электронный ресурс]. — Режим доступа: https://top10-sed.ru/.