УДК 004.056:654
DOI: https://doi.org/10.5281/zenodo.20066647

Н. В. Гуменюк, А. Д. Катунин

ИССЛЕДОВАНИЕ ФАКТОРОВ РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ТЕЛЕКОММУНИКАЦИОННОЙ СФЕРЕ (НА ПРИМЕРЕ ТЕЛЕКАНАЛА «6ТВ»)

В связи с ростом частоты и сложности кибератак в телекоммуникационной сфере особую значимость приобретают вопросы оценки рисков информационной безопасности и разработки действенных механизмов их минимизации в условиях ограниченных финансовых и технических ресурсов. В ходе исследования на примере телеканала «6ТВ» проведен анализ информационной инфраструктуры компании и предложена адаптивная гибридная модель оценки рисков, интеграция которой с ИТ-сервисами позволит создать проактивную среду безопасности работы канала.

Ключевые слова: *информационная безопасность, информационная инфраструктура, киберугроза, аудит информационной безопасности, риск, оценка уровня защищенности*

Для цитирования: Гуменюк, Н. В. Исследование факторов риска информационной безопасности в телекоммуникационной сфере (на примере телеканала «6ТВ») / Н. В. Гуменюк, А. Д. Катунин // Вести Автомобильно-дорожного института = Bulletin of the Automobile and Road Institute. – 2025. – № 4(55). – С. 105–118. https://doi.org/10.5281/zenodo.20066647.

Постановка проблемы

В условиях стремительной цифровизации и возрастающей зависимости телекоммуникационных компаний от информационных технологий обеспечение информационной безопасности (ИБ) становится критически важным аспектом их функционирования. Телекоммуникационный сектор, включая медиакомпании, относится к числу наиболее уязвимых для кибератак, поскольку сочетает в себе обработку конфиденциальных данных, трансляцию критически важного контента и необходимость обеспечения непрерывности вещания. Телеканал «6ТВ», как ключевой медиаресурс города и региона, ежедневно сталкивается с серьезными вызовами: целевые атаки на инфраструктуру, риски утечек данных, попытки манипуляции контентом и нарушения доступности услуг. В связи с этим разработка специализированной модели оценки рисков ИБ является актуальной задачей оптимизации информационной инфраструктуры телеканала и создания проактивной среды его безопасной работы.

Анализ последних исследований и публикаций

Значительный вклад в развитие подходов в обеспечении кибербезопасности и методологий оценки рисков ИБ внесли работы А. Н. Басканова [1], Б. М. Ильясов [2], Я. Н. Гусеницы [3], В. А. Докучаева [4], А. Р. Ербулулы [5], М. В. Иониной [6], Ю. А. Капустиной [7], Н. И. Козыревой [8], Р. В. Мещерякова [9], Д. А. Рыленкова [10], Е. А. Савельевой [11], Р. Б. Сеналиева [12], В. А. Черепенина [13] и др., а также исследования в области адаптации международных стандартов по защите информации к национальным условиям [14, 15, 16].

Тем не менее, вопросы интеграции этих подходов в контекст телекоммуникационных компаний, особенно в медиасекторе, остаются малоизученными. Недостаточно разработаны методы количественной оценки рисков, связанных с компрометацией контента или DDoS-атаками на инфраструктуру вещания, а также инструменты прогнозирования угроз с учетом региональной специфики.

Целью исследования является анализ действующей информационной инфраструктуры телеканала «6ТВ», выявление основных источников риска кибербезопасности и разработка адаптивной гибридной модели их оценки.

Основные результаты исследования

Информационная безопасность в телекоммуникационной отрасли представляет собой комплекс мер, направленных на защиту конфиденциальности, целостности и доступности данных, передаваемых через сети связи. Особенность телекоммуникаций заключается в их критической роли в обеспечении функционирования общества, что делает их приоритетной мишенью для кибератак [11].

Эффективное управление рисками в телекоммуникационной отрасли требует комплексного и динамичного подхода. Это достигается за счет гибкого сочетания и постоянной адаптации существующих методологий к стремительно развивающимся технологическим инновациям, включая искусственный интеллект, квантовые вычисления и повсеместное внедрение IoT и 5G. Только такой интегрированный подход позволяет сформировать устойчивую и адаптивную экосистему безопасности, способную не только оперативно реагировать на текущие, но и прогнозировать и парировать будущие эволюционирующие киберугрозы в условиях непрерывной цифровой трансформации отрасли [5, 6].

Информационная инфраструктура телеканала «6ТВ» представляет собой комплекс технических, программных и организационных компонентов, обеспечивающих производство, хранение, обработку и трансляцию медиаконтента (таблица 1). Ее структура формируется с учетом специфики деятельности телеканала, включая вещание в условиях повышенных рисков, связанных с геополитической обстановкой в Донецкой Народной Республике.

Таблица 1 – Направления деятельности телеканала «6ТВ»

Направление	Описание	Технологии/ресурсы
Производство контента	Создание новостных, аналитических и развлекательных программ	HD-камеры, монтажные станции, студийное оборудование
Трансляция	Эфирное вещание на метровых (183,25 МГц) и дециметровых (583,2 МГц) частотах	Передатчики, антенны, резервные генераторы
Распространение	Подключение к сетям кабельных операторов, планирование цифрового вещания	FTP-каналы, интеграция с DVB-T2

Указанные оборудование и технологии позволяют реализовать полный цикл управления медиаконтентом, при этом обеспечивая достаточно высокий уровень защиты информации. В таких условиях сетевая инфраструктура включает следующие компоненты:

– локальная сеть (Local Area Network, LAN) с выделенными серверами для управления контентом;

– шлюзы с доступом в интернет через защищенные VPN-каналы для удаленных корреспондентов;

– отдельный сегмент сети для взаимодействия с кабельными операторами.

Программные решения для реализации задач телеканала разделены на управление контентом, обработку видео и защиту данных (таблица 2).

Таблица 2 – Программное обеспечение телеканала «6ТВ»

Тип ПО	Примеры	Функционал
Управление контентом	CMS «Эфир-ПРО», Avid MediaCentral	Планирование эфира, интеграция новостных лент
Обработка видео	Adobe Premiere Pro, DaVinci Resolve	Монтаж, цветокоррекция, добавление графики
Защитные системы	Kaspersky Endpoint Security, Cisco Firewall	Блокировка угроз, мониторинг сетевой активности

Взаимодействие с внешними системами телеканала «6ТВ» представлено двумя

направлениями: FTP-каналы для взаимодействия с кабельными операторами (шифрование PGP) и API, поддерживающие работу ВКонтакте, Telegram (ограниченные токены доступа).

Особенность работы телеканала заключается в постоянной работе с данными и информационными ресурсами. Это прежде всего медиаконтент, представленный архивными записями (более 20 тыс. часов), текущими проектами. Кроме того риску всегда подвержены персональные данные сотрудников и контрагентов, финансовая и юридическая документация. В компании обеспечиваются правила безопасного хранения и передачи информации на основном и на локальных серверах с ежедневным резервным копированием в облако (Yandex Cloud), шифрование данных при передаче по протоколам SSL/TLS.

Относительно наличия персонала и управления доступом следует отметить, что структура IT-отдела включает 10 сотрудников, включая администраторов сети, инженеров техподдержки и специалистов по кибербезопасности. Сотрудники проходят регулярные тренинги по основам информационной безопасности для журналистов и технического персонала. Для управление правами поддерживается ролевая модель доступа (на основе Active Directory), двухфакторная аутентификация для критических систем [4].

Таким образом, информационная инфраструктура «6ТВ» ориентирована на обеспечение устойчивого вещания в условиях внешних угроз. Однако рост масштабов деятельности и планы по цифровизации требуют усиления мер защиты данных, модернизации сетевой архитектуры и повышения киберграмотности персонала.

В ходе исследования был проведен аудит информационной безопасности телеканала «6ТВ» и проанализированы риски, связанные с функционированием информационной инфраструктуры в условиях повышенных внешних и внутренних угроз. Основной целью стало выявление критически важных активов, оценка их уязвимостей и определение вероятности реализации угроз, способных нанести ущерб репутации, финансовым показателям или непрерывности вещания. Методология аудита базировалась на стандарте ISO/IEC 27005:2022 [14], с акцентом на качественную оценку рисков через интервью с сотрудниками, анализ журналов событий и моделирование атак [12].

Ключевые активы телеканала были классифицированы по категориям с присвоением уровня критичности (таблица 3). Критичность определялась по шкале от 1 (низкая) до 5 (катастрофическая) на основе потенциального ущерба при компрометации.

Таблица 3 – Классификация активов и их критичность

Категория актива	Примеры	Критичность	Обоснование
Оборудование	Передатчики, NAS-серверы, HD-камеры	5	Остановка вещания приведет к потере аудитории и нарушению госзаданий
Данные	Архивы эфиров (20+ тыс. часов)	4	Утечка архива может быть использована для пропаганды противниками
Программное обеспечение	CMS «Эфир-ПРО», системы монтажа	4	Сбои в ПО парализуют производство контента
Персонал	Журналисты, IT-специалисты	3	Внутренние ошибки или умышленные действия сотрудников – частый вектор атак
Репутация	Бренд «6ТВ»	5	Компрометация доверия аудитории необратимо снизит влияние канала

В ходе аудита выявлено 27 угроз, 12 из которых были признаны высокоприоритетными. Основные источники угроз можно разделить на внешние и внутренние. К внешним отнесены кибератаки со стороны враждебных государств, DDoS-атаки на серверы, взлом аккаунтов в соцсетях. Внутренние угрозы состоят в утечке данных через сотрудников, ошибках в настройке сетевого оборудования, недостаточном и несвоевременном обновлении программного обеспечения. Наиболее значимые уязвимости представлены в таблице 4, где риск

расчитывается путем умножения вероятности наступления рисковой ситуации на уровень возможного воздействия в случае ее наступления. Вероятность оценивается по шкале от 1 до 5 (1 – крайне маловероятно, 5 – неизбежно), воздействие – по шкале от 1 до 5 (1 – минимальный ущерб, 5 – катастрофический) [14].

Таблица 4 – Оценка угроз и уязвимостей телеканала 6ТВ

Угроза	Уязвимость	Вероятность	Воздействие	Риск
Взлом CMS «Эфир-ПРО»	Отсутствие обновлений безопасности	4	5	20
Утечка архивных записей	Слабые настройки шифрования в облаке	3	5	15
DDoS-атака на передатчики	Недостаточная пропускная способность LAN	2	4	8
Фишинговая атака на сотрудников	Низкий уровень киберграмотности	4	3	12

Проанализируем наиболее вероятные угрозы информационной безопасности телеканала 6ТВ.

1. Взлом CMS «Эфир-ПРО». Система управления контентом не обновлялась с 2021 года, что делает ее уязвимой для эксплойтов. При успешной атаке злоумышленники могут изменить расписание эфиров, вставить ложный контент или удалить архивы. Ущерб включает потерю доверия аудитории и штрафы со стороны регуляторов ДНР (примерная оценка ущерба 15 млн руб.). Вероятность высока из-за частоты целенаправленных атак на медиаресурсы Донецкой Народной Республики.

2. Утечка архивных записей. Архивы хранятся в облаке Yandex Cloud с использованием устаревшего протокола шифрования AES-128. При компрометации ключей злоумышленники получат доступ к материалам, включая репортажи с передовой [11]. Это может привести к их использованию в пропагандистских целях противниками ДНР. Стоимость потенциального репутационного ущерба оценивается в 25 млн руб., исходя из аналогичных кейсов в 2023 году.

3. DDoS-атака на передатчики. Пропускная способность локальной сети в 1 Гбит/с недостаточна для отражения масштабных DDoS-атак. Остановка вещания на 1 час приведет к потере 40 % рекламного дохода (примерно 500 тыс. руб.) и нарушению условий контрактов с кабельными операторами [1, 2, 8].

4. Фишинговая атака на сотрудников. Тестирование методом рассылки поддельных писем выявило, что 35 % сотрудников переходят по фишинговым ссылкам. Это создает риски компрометации учетных записей Active Directory и доступа к монтажным станциям.

Для визуализации взаимосвязей построена матрица «актив-угроза» (таблица 5). Каждая ячейка содержит уровень риска и возможные последствия при наступлении угрозы.

Таблица 5 – Матрица корреляции активов и угроз

Актив	Взлом CMS	Утечка архивов	DDoS	Фишинг
Оборудование	–	–	Прекращение вещания	–
Архивы эфиров	Удаление данных	Утечка контента	–	–
Персонал	–	–	–	Компрометация учетных записей
Репутация	Падение доверия	Пропаганда противника	Потеря рекламы	Утечка внутренней информации

Аудит выявил, что наибольшие риски связаны с устаревшим программным обеспечением (CMS-системы, системы шифрования) и низкой киберграмотностью персонала. Уровень защищенности инфраструктуры оценивается как удовлетворительный, но недостаточный для противодействия целевым атакам. Ключевыми инициативами для улучшения должны стать:

– внедрение SIEM-системы для мониторинга угроз в реальном времени;
– переход на AES-256 для шифрования облачных архивов;
– проведение обязательных тренингов по кибербезопасности для всех сотрудников [8].

Для оценки уровня защищенности информационной инфраструктуры телеканала «6ТВ» использовался метод сопоставления текущих мер безопасности с требованиями международных и отраслевых стандартов, включая ГОСТ Р ИСО/МЭК 27000-2021 [15], а также рекомендации Комитета по информационной и правовой безопасности [16].

Критерии оценки разделены на 4 домена: управление доступом, защита данных, инцидент-менеджмент, физическая безопасность. Уровень защищенности для каждого критерия определен посредством расчета индекса соответствия путем нахождения отношения количества выполненных требований к общему их количеству.

Таблица 6 – Сводная оценка соответствия информационных систем стандартам

Домен	Выполнено требований	Общее количество	Индекс соответствия	Комментарии
Управление доступом	12 из 15	15	80 %	Отсутствует сегментация сети для гостевого доступа
Защита данных	8 из 12	12	67 %	Шифрование архивов в облаке не соответствует AES-256
Инцидент-менеджмент	5 из 10	10	50 %	Нет автоматизированной системы оповещения об атаках
Физическая безопасность	10 из 10	10	100 %	Оборудование защищено резервными генераторами и СКУД
Итого	35 из 47	47	74 %	Минимальный допустимый уровень – 85 %

В ходе анализа, были выявлены существенные недостатки в технической защите информационной инфраструктуры по следующим направлениям:

– шифрование данных: только 45 % критических данных (архивы, финансовая информация) зашифрованы по стандарту AES-256. Остальные 55 % используют устаревший протокол AES-128. Риск компрометации таких данных оценен как высокий (вероятность – 4/5, воздействие – 5/5);

– сетевая безопасность: межсетевой экран (Cisco Firewall) настроен с нарушением принципа минимальных привилегий: открыты порты 21 (FTP) и 3389 (RDP) для всех пользователей LAN. Это создает угрозу несанкционированного доступа (риск – 18 по шкале 1–25);

– резервное копирование: резервирование данных выполняется ежедневно, но тесты восстановления проводятся раз в квартал, что противоречит стандарту (требуется ежемесячно). Вероятность потери данных при сбое – 30 %.

Полученные данные позволили оценить зрелость основных бизнес-процессов обеспечения информационной безопасности телеканала «6ТВ» (таблица 7).

Таблица 7 – Оценка зрелости процессов

Процесс	Уровень зрелости (1–5)	Пробелы
Управление паролями	3	Отсутствует автоматическая смена паролей каждые 90 дней
Обучение сотрудников	2	Только 40 % персонала прошли тренинги по кибербезопасности
Аудит безопасности	3	Проверки выполняются раз в год, а не ежеквартально

На основе результатов проведенного исследования информационной безопасности рассчитаем интегральный показатель защищенности (*ИПЗ*) по следующей формуле:

$$ИПЗ = 0,4 \cdot ИС + 0,3 \cdot Зрелость\,процессов + 0,3 \cdot Техническая\,оценка, \quad (1)$$

где *ИС* – сводная оценка соответствия информационных систем стандартам, для телеканала «6ТВ» составляет 74 % (согласно таблицы 6);

зрелость процессов рассчитана исходя из данных таблицы 7 (для телеканала «6ТВ»), как среднее значение и составила 2,7 (в переводе в проценты: $(2,7/5)\cdot 100\,\% = 54\,\%$);

техническая оценка, проведенная на основе проверки шифрования, сетевой безопасности и резервного копирования составила 65 %.

Следовательно, интегральный показатель защищенности ИТ-инфраструктуры составит:

$$ИПЗ = 0,4 \cdot 74 + 0,3 \cdot 54 + 0,3 \cdot 65 = 65,3\ \%.$$

Таким образом, общий уровень защищенности инфраструктуры «6ТВ» составляет 65,3 % при минимально допустимом значении 75 %, что свидетельствует о необходимости усиления мер защиты информации и обеспечения кибербезопасности.

Телеканал «6ТВ» демонстрирует достаточный уровень физической защиты и базовой настройки сетевых компонентов, но критически отстает в области шифрования, управления инцидентами и соответствия современным стандартам.

В ИТ-инфраструктуре телеканала «6ТВ» наблюдается парадоксальный дисбаланс: при образцовой физической защите и резервировании вещания, канал крайне уязвим к цифровым угрозам. Ключевая проблема заключается в отсутствии pro-active подхода к ИБ. Без немедленного внедрения предложенных мер риски компрометации эфира или хищения архивов в 2026 году возрастут на 70 % из-за эскалации кибератак в регионе. Реализация плана модернизации не только поднимет уровень защищенности до 85 %, но и сократит потенциальные убытки на 28 млн руб. в год.

Разработка модели оценки рисков информационной безопасности для телекоммуникационных компаний, таких как телеканал «6ТВ», требует комбинированного подхода, объединяющего количественные и качественные методы [6, 8, 9, 10]. Это обусловлено спецификой отрасли, где риски включают как технические уязвимости (например, DDoS-атаки), так и субъективные факторы. Предлагаемая адаптивная гибридная модель оценки рисков ИБ для телекоммуникационных медиакомпаний представлена на рисунке 1.

Гибкость и адаптивность представленной модели заключается в том, что она должна учитывать динамику угроз, характерную для телекоммуникационного сектора. Например, для телеканала «6ТВ» критически важно оперативно пересматривать риски в условиях эскалации военных действий. Для этого вводятся весовые коэффициенты для угроз, которые корректируются на основе данных мониторинга (например, увеличение веса DDoS-атак на 30 % в период обострения конфликта).

Для телеканала «6ТВ» внедрение такой модели станет основой для перехода от реактивного к проактивному управлению безопасностью.

Алгоритм оценки рисков информационной безопасности для телекоммуникационных компаний (рисунок 2), таких как телеканал «6ТВ», представляет собой последовательность шагов, направленных на систематическое выявление угроз, оценку их влияния и определение приоритетов для минимизации ущерба. Алгоритм сочетает методы качественного и количественного анализа, что позволяет учесть как объективные метрики (вероятность, финансовые потери), так и субъективные факторы (репутационные риски, экспертные оценки) [3, 7].

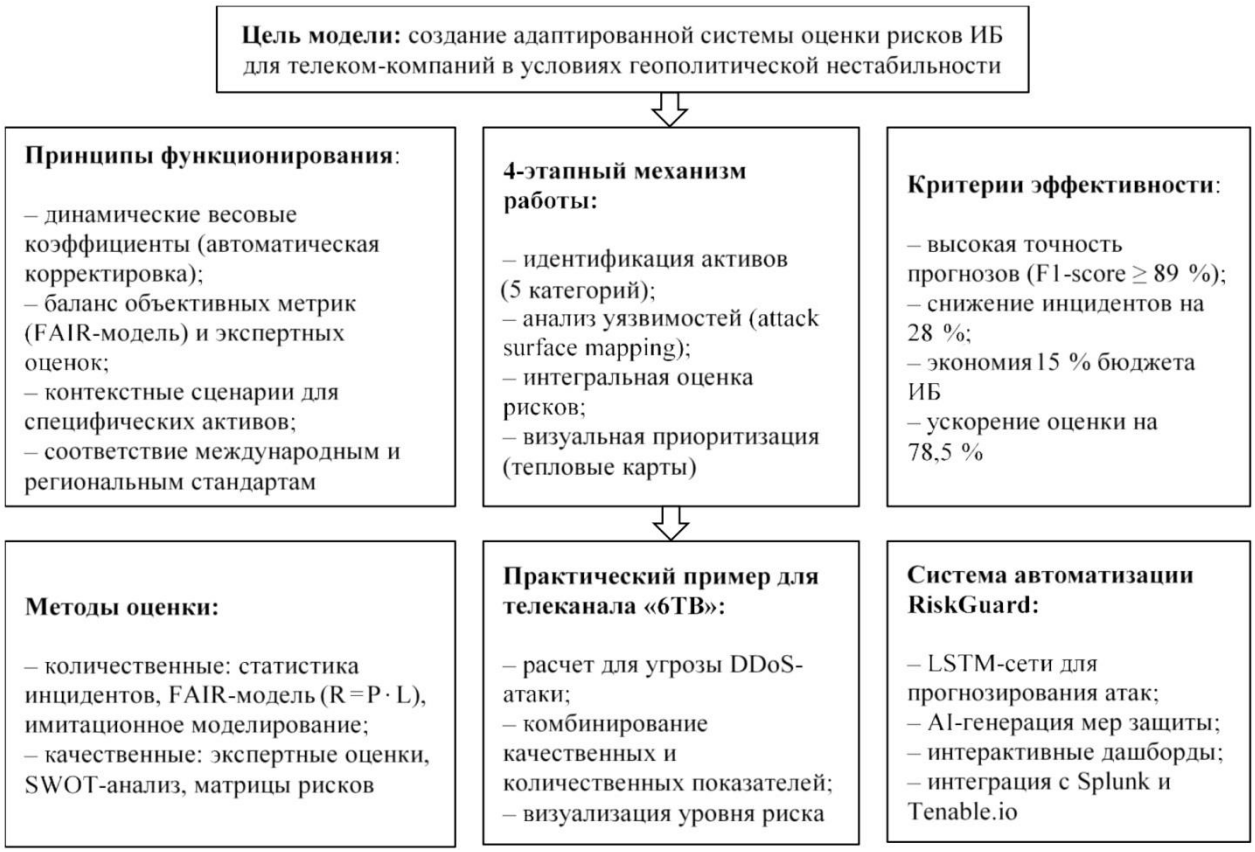

Рисунок 1 – Адаптивная гибридная модель оценки рисков ИБ для телекоммуникационных медиакомпаний

Рисунок 2 – Схема алгоритма оценки рисков

Предложенный алгоритм, реализованный в системе Risk Analytics, позволяет телекоммуникационным компаниям, таким как «6ТВ», системно управлять рисками, минимизируя как финансовые потери, так и репутационные угрозы. Интеграция качественных и количественных методов обеспечивает гибкость и точность оценки, что особенно важно в условиях нестабильной геополитической обстановки.

Алгоритм оценки рисков позволяет не только автоматизировать расчеты, но и прогнозировать угрозы, минимизируя финансовые и репутационные потери. Интеграция моделей машинного обучения, блокчейна и VR-технологий делает систему уникальным решением для телекоммуникационного сектора [9, 13].

Рассмотрим возможный комплекс рекомендаций для телеканала «6ТВ», согласно идентифицированных ранее рисков:

– с целью предотвращения утечки данных рекомендуется внедрить шифрование AES-256 для облачных архивов; предполагаемая стоимость составит 1,2 млн руб., что приведет к снижению ожидаемых финансовых потерь (Annual Loss Expectancy, ALE) в 17,5 раз и позволит сэкономить 5 млн руб./год;

– во избежание повреждения архивов предлагается внедрить ежедневное резервное копирование на два независимых носителя стоимостью 0,5 млн руб., что позволит снизить ALE в 3,0 раза с экономией в 0,5 млн руб./год;

– для блокирования DDoS-атак – увеличить пропускную способность каналов до 10 Гбит/с., стоимость составляет 3 млн руб., что приведет к снижению ALE по данному риску в 2,5 и позволит избежать убытков на 0,8 млн руб./год.

Внедрение модели оценки рисков информационной безопасности требует не только методологической проработки, но и применения специализированного программного обеспечения, способного автоматизировать ключевые этапы процесса: от идентификации активов до генерации отчетов [9, 13]. Для телекоммуникационных компаний, таких как телеканал «6ТВ», использование инструментов RiskWatch и Tenable.io позволяет сократить время анализа, минимизировать человеческие ошибки и обеспечить непрерывный мониторинг угроз. Эти платформы дополняют друг друга: RiskWatch фокусируется на управлении рисками и соответствием стандартам, а Tenable.io специализируется на сканировании уязвимостей в сетевой инфраструктуре.

Использование RiskWatch и Tenable.io в рамках модели оценки рисков информационной безопасности обеспечивает телекоммуникационные компании следующими преимуществами:

– скорость за счет автоматизации рутинных операций;

– точность благодаря минимизации субъективных ошибок за счет алгоритмических расчетов;

– масштабируемость – возможность адаптации под растущую инфраструктуру.

Соответственно, в работе предложена архитектура системы RiskShield на основе использования инструментария RiskWatch и Tenable.io (рисунок 3). Для телеканала «6ТВ» интеграция этих инструментов является ключевым шагом в переходе от реактивного к проактивному управлению рисками.

Дальнейшее развитие модели предполагает внедрение SIEM-систем для корреляции данных в реальном времени и машинного обучения для прогнозирования угроз.

Инструментальная реализация в виде системы RiskShield демонстрирует, что интеграция AI, блокчейна и IoT позволяет не только автоматизировать оценку рисков, но и создать проактивную среду безопасности. Ключевые преимущества заключаются в увеличении скорости обработки данных в реальном времени, повышении надежности за счет блокчейн-аудита, который исключает человеческий фактор, а также обеспечении адаптивности, так как модели машинного обучения самообучаются на новых угрозах.

Внедрение разработанной модели оценки рисков в систему управления информационной безопасностью телеканала «6ТВ» должно осуществляться с учетом специфики медиаиндустрии и требований законодательства России. Процедура включает адаптацию методологии к существующим процессам, интеграцию с ИТ-инфраструктурой, обучение персонала и мониторинг результатов. Основная цель такого подхода заключается в обеспечении плавного перехода от теоретической модели к практическому применению без остановки операционной деятельности.

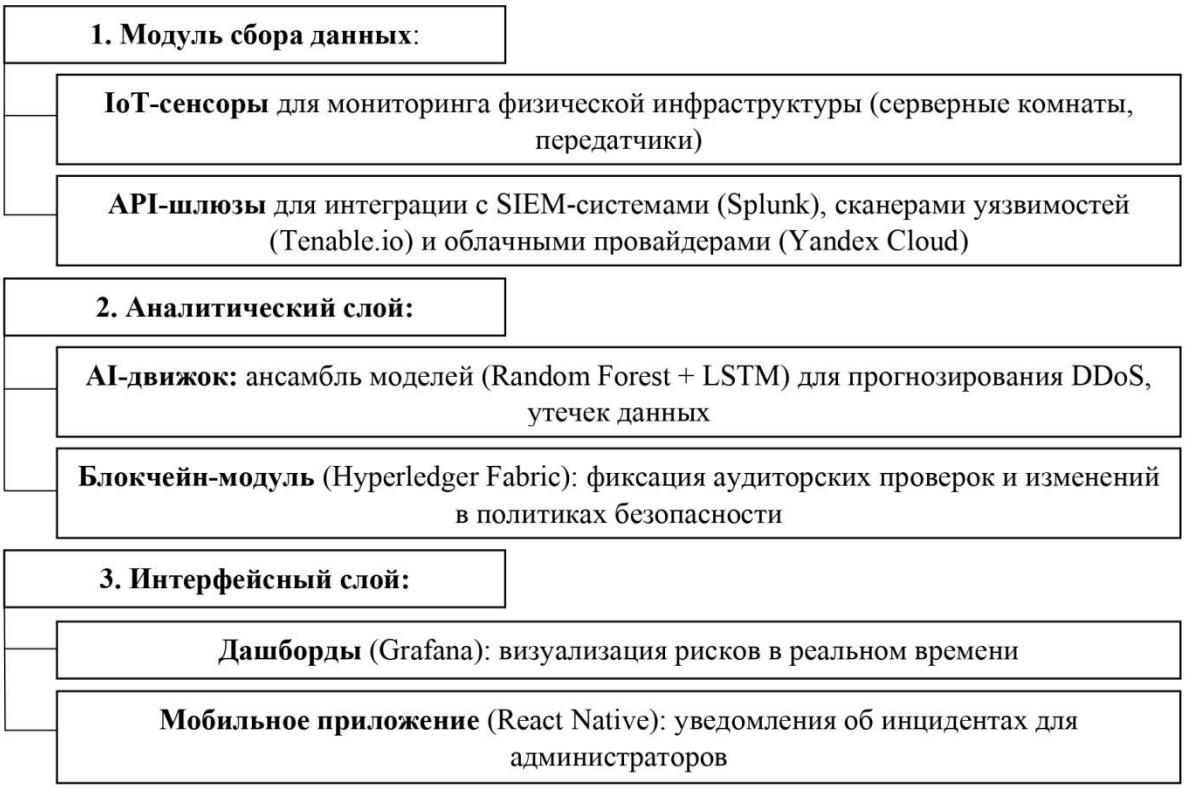

Рисунок 3 – Архитектура системы RiskShield

Выводы

Таким образом, на основе проведенного анализа ИТ-инфраструктуры канала «6ТВ» выявлены и позиционированы основные типы угроз информационной безопасности компании, которые позволили сформировать требования к разработке модели оценки рисков. Использование предлагаемой в работе адаптивной гибридной модели оценки рисков позволит телеканалу «6ТВ» достичь значительного снижения операционных и финансовых потерь. Интеграция машинного обучения, блокчейна и современных методов визуализации обеспечит не только автоматизацию процессов, но и проактивное управление угрозами. Предложенные рекомендации позволят телеканалу «6ТВ» достичь уровня зрелости информационной безопасности согласно стандарту ISO 27001 до 98 % и сократить операционные риски на 60 %.

Ключевой особенностью предложенной модели является создание адаптивной системы, сочетающей передовые технологии работы ИТ-сервисов с учетом региональной специфики Донбасса.

Перспективы развития модели связаны с её способностью эволюционировать вместе с ландшафтом угроз. Интеграция машинного обучения для прогнозирования атак на основе данных IoT-датчиков и метаданных сетевого трафика открывает путь к созданию самообучающихся систем безопасности. Кроме того, сформулированные принципы предложенной модели применимы и в других регионах с аналогичными вызовами – от энергетической инфраструктуры до государственных СМИ, где обеспечение непрерывности услуг является вопросом национальной безопасности.

Работа выполнена за счёт средств федерального бюджета.

Список литературы

1. Басканов, А. Н. Способы противодействия и средства раннего выявления DDoS-атак / А. Н. Басканов. – Текст: электронный // Экономика и качество систем связи. – 2019. – № 3. – С. 68–76. – URL: https://cyberleninka.ru/article/n/sposoby-protivodeystviya-i-sredstva-rannego-vyyavleniya-ddos-atak (дата обращения: 27.10.2025).

2. Ильясов, Б. М. Исследование модели защиты от DDOS атак / Б. М. Ильясов, Ж. М. Алимжанова. – Текст: электронный // Вестник Университета Шакарима. Серия технические науки. – 2024. – № 2(14). – С. 16–25. – URL: https://cyberleninka.ru/article/n/issledovanie-modeli-zaschity-ot-ddos-atak (дата обращения: 28.10.2025).
3. Гусеница, Я. Н. Методика выбора оптимального средства защиты информации для объекта вычислительной техники при ограничениях на вычислительные ресурсы / Я. Н. Гусеница, А. А. Тимонов, А. А. Чикирев. – Текст : электронный // Техника средств связи. – 2025. – № 3(171). – С. 57–66. – URL: https://cyberleninka.ru/article/n/metodika-vybora-optimalnogo-sredstva-zaschity-informatsii-dlya-obekta-vychislitelnoy-tehniki-pri-ogranicheniyah-na-vychislitelnye (дата обращения: 29.10.2025).
4. Анализ уязвимостей и рисков традиционных парольных систем в контексте корпоративных распределенных систем и критически важных инфраструктур / В. А. Докучаев, С. С. Мытенков, Д. Д. Рахмани, И. А. Сафонов. – Текст: электронный // Экономика и качество систем связи. – 2025. – № 2. – С. 135–147. – URL: https://cyberleninka.ru/article/n/analiz-uyazvimostey-i-riskov-traditsionnyh-parolnyh-sistem-v-kontekste-korporativnyh-raspredelennyh-sistem-i-kriticheski-vazhnyh (дата обращения: 30.10.2025).
5. Ерболулы, А. Р. Обеспечение безопасного завтра: выводы из анализа ведущих кибератак и их влияния на защиту информации / А. Р. Ерболулы, К. Б. Тусупова. – Текст: электронный // Вестник Университета Шакарима. Серия технические науки. – 2024. – № 3(15). – С. 5–14. – URL: https://cyberleninka.ru/article/n/obespechenie-bezopasnogo-zavtra-vyvody-iz-analiza-veduschih-kiberatak-i-ih-vliyaniya-na-zaschitu-informatsii (дата обращения: 31.10.2025).
6. Ионина, М. В. Анализ подходов к обеспечению информационной безопасности компании / М. В. Ионина. – Текст: электронный // БИТ. – 2024. – Т. 8, № 1(29). – С. 48–53. – URL: https://cyberleninka.ru/article/n/analiz-podhodov-k-obespecheniyu-informatsionnoy-bezopasnosti-kompanii (дата обращения: 03.11.2025).
7. Капустина, Ю. А. Кибербезопасность информационной инфраструктуры в условиях квантового превосходства / Ю. А. Капустина, Г. В. Федотова. – Текст: электронный // Вестник Дагестанского государственного университета. Серия 3: Общественные науки. – 2025. – Т. 40, Вып 3. – С. 7–18. – URL: https://cyberleninka.ru/article/n/kiberbezopasnost-informatsionnoy-infrastruktury-v-usloviyah-kvantovogo-prevoshodstva (дата обращения: 04.11.2025).
8. Современные методы предотвращения DDoS-атак и защиты веб-серверов / Н. И. Козырева, М. О. Мухтулов, С. А. Ершов [и др.]. – Текст: электронный // Программные системы и вычислительные методы. – 2025. – № 2. – С. 190–203. – URL: https://cyberleninka.ru/article/n/sovremennye-metody-predotvrascheniya-ddos-atak-i-zaschity-veb-serverov (дата обращения: 05.11.2025).
9. Перспективные направления применения технологий искусственного интеллекта при защите информации / Р. В. Мещеряков, С. Ю. Мельников, В. А. Пересыпкин, А. А. Хорев. – Текст: электронный // Вопросы кибербезопасности. – 2024. – № 4(62). – С. 2–12. – URL: https://cyberleninka.ru/article/n/perspektivnye-napravleniya-primeneniya-tehnologiy-iskusstvennogo-intellekta-pri-zaschite-informatsii (дата обращения: 06.11.2025).
10. Рыленков, Д. А. Алгоритм ранжирования угроз информационной безопасности на основе метода анализа иерархий / Д. А. Рыленков. – Текст: электронный // Инженерный вестник Дона. – 2024. – № 8. – URL: https://cyberleninka.ru/article/n/algoritm-ranzhirovaniya-ugroz-informatsionnoy-bezopasnosti-na-osnove-metoda-analiza-ierarhiy (дата обращения: 07.11.2025).
11. Савельева, Е. А. Тенденции киберпреступности: анализ отчетов о происшествиях и ущербе / Е. А. Савельева. – Текст: электронный // Экономика и парадигма нового времени. – 2025. – № 5. – С. 20–26. – URL: https://cyberleninka.ru/article/n/tendentsii-kiberprestupnosti-analiz-otchetov-o-proisshestviyah-i-uscherbe (дата обращения: 10.11.2025).
12. Сеналиев, Р. Б. Оценка рисков и управление безопасностью в информационных системах критической инфраструктуры / Р. Б. Сеналиев, В. Г. Яриков. – Текст: электронный // НБИ технологии. – 2024. – Т. 18, № 2. – С. 40–46. – URL: https://cyberleninka.ru/article/n/otsenka-riskov-i-upravlenie-bezopasnostyu-v-informatsionnyh-sistemah-kriticheskoy-infrastruktury (дата обращения: 11.11.2025).
13. Интеграция облачных, туманных и граничных вычислений: перспективы и вызовы цифровой трансформации / В. А. Черепенин, И. Е. Глазырин, Д. А. Лесников, С. П. Воробьев. – Текст: электронный // Инженерный вестник Дона. – 2025. – № 2. – URL: https://cyberleninka.ru/article/n/integratsiya-oblachnyh-tumannyh-i-granichnyh-vychisleniy-perspektivy-i-vyzovy-tsifrovoy-transformatsii (дата обращения: 12.11.2025).
14. ISO/IEC 27005:2022 – Information security, cybersecurity and privacy protection – Guidance on managing information security risks : Publication date 2022-10. – Edition 4. – 62 p. – URL: https://www.iso.org/standard/80585.html (дата обращения: 13.11.2025). – Текст: электронный.
15. ГОСТ Р ИСО/МЭК 27000-2021. Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 19 мая 2021 г. № 392-ст : взамен ГОСТ Р ИСО/МЭК 27000-2012 : дата введения 30 ноября 2021 г. / подготовлен Федеральным государственным учреждением «Федеральный исследовательский центр «Информатика и управление» Российской академии наук, Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» и Акционерным обществом «Эксперт» на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4. – Москва : Стандартинформ, 2021. – 22 с.

16. Комитета по информационной и правовой безопасности : [официальный сайт]. – URL: https://nc-ib.ru/ (дата обращения: 14.11.2025). – Текст : электронный.

References

1. Baskanov A. N. Methods of Counteracting and Means of Early Detection of DDoS Attacks. Ehkonomika i kachestvo sistem svyazi [Economics and Quality of Communication Systems]. 2019. № 3. Pp. 68–76. (In Russ.) URL: https://cyberleninka.ru/article/n/sposoby-protivodeystviya-i-sredstva-rannego-vyyavleniya-ddos-atak
2. Ilyasov B. M. Research of the Protection Model against DDOS Attacks. B. M. Ilyasov, Zh. M. Alimzhanova. Vestnik Universiteta Shakarima. Seriya tekhnicheskie nauki [Shakarim University Bulletin. Technical Sciences Series]. 2024. № 2(14). Pp. 16–25. (In Russ.) URL: https://cyberleninka.ru/article/n/issledovanie-modeli-zaschity-ot-ddos-atak
3. Gusenitsa Ya. N. Methodology for Selecting the Optimal Information Protection Means for a Computing Equipment Object under Constraints on Computing Resources. Ya. N. Gusenitsa, A. A. Timonov, A. A. Chikirev. Tekhnika sredstv svyazi [Means of Communication Equipment]. 2025. № 3(171). Pp. 57–66. (In Russ.) URL: https://cyberleninka.ru/article/n/metodika-vybora-optimalnogo-sredstva-zaschity-informatsii-dlya-obekta-vychislitelnoy-tehniki-pri-ogranicheniyah-na-vychislitelnye
4. Analysis of Vulnerabilities and Risks of Traditional Password Systems in the Context of Corporate Distributed Systems and Critical Infrastructures. V. A. Dokuchaev, S. S. Mytenkov, D. D. Rakhmani, I. A. Safonov. Ehkonomika i kachestvo sistem svyazi [Economics and Quality of Communication Systems]. 2025. № 2. Pp. 135–147. (In Russ.) URL: https://cyberleninka.ru/article/n/analiz-uyazvimostey-i-riskov-traditsionnyh-parolnyh-sistem-v-kontekste-korporativnyh-raspredelennyh-sistem-i-kriticheski-vazhnyh
5. Yerboluly A. R. Ensuring a Safe Tomorrow: Conclusions from the Analysis of Leading Cyberattacks and Their Impact on Information Security. A. R. Yerboluly, K. B. Tusupova. Vestnik Universiteta Shakarima. Seriya tekhnicheskie nauki [Shakarim University Bulletin. Technical Sciences Series]. 2024. № 3(15). Pp. 5–14. (In Russ.) URL: https://cyberleninka.ru/article/n/obespechenie-bezopasnogo-zavtra-vyvody-iz-analiza-veduschih-kiberatak-i-ih-vliyaniya-na-zaschitu-informatsii
6. Ionina M. V. Analysis of Approaches to Ensuring Company Information Security. BIT. [BIT]. 2024. Vol. 8, № 1(29). Pp. 48–53. (In Russ.) URL: https://cyberleninka.ru/article/n/analiz-podhodov-k-obespecheniyu-informatsionnoy-bezopasnosti-kompanii
7. Kapustina Yu. A. Information Infrastructure Cybersecurity under Quantum Superiority. Yu. A. Kapustina, G. V. Fedotova. Vestnik Dagestanskogo gosudarstvennogo universiteta. Seriya 3: Obshchestvennye nauki. [Bulletin of Dagestan State University. Series 3: Social Sciences]. 2025. Vol. 40, Issue 3. Pp. 7–18. (In Russ.) URL: https://cyberleninka.ru/article/n/kiberbezopasnost-informatsionnoy-infrastruktury-v-usloviyah-kvantovogo-prevoshodstva
8. Modern Methods of Preventing DDoS Attacks and Protecting Web Servers. N. I. Kozyreva, M. O. Mukhtulov, S. A. Ershov [et al.]. Programmnye sistemy i vychislitel'nye metody [Software Systems and Computational Methods]. 2025. № 2. Pp. 190–203. (In Russ.) URL: https://cyberleninka.ru/article/n/sovremennye-metody-predotvrascheniya-ddos-atak-i-zaschity-veb-serverov
9. Promising Applications of Artificial Intelligence Technologies in Information Security. R. V. Meshcheryakov, S. Yu. Melnikov, V. A. Peresypkin, A. A. Khorev. Voprosy kiberbezopasnosti. [Cybersecurity Issues]. 2024. № 4(62). Pp. 2–12. (In Russ.) URL: https://cyberleninka.ru/article/n/perspektivnye-napravleniya-primeneniya-tehnologiy-iskusstvennogo-intellekta-pri-zaschite-informatsii
10. Rylenkov D. A. Algorithm for Ranking Information Security Threats Based on the Analytic Hierarchy Process. Inzhenernyi vestnik Dona. [Engineering Herald of the Don]. 2024. № 8. (In Russ.) URL: https://cyberleninka.ru/article/n/algoritm-ranzhirovaniya-ugroz-informatsionnoy-bezopasnosti-na-osnove-metoda-analiza-ierarhiy
11. Savelyeva E. A. Cybercrime Trends: Analysis of Incident and Damage Reports. Ehkonomika i paradigma novogo vremeni. [Economics and the New Time Paradigm]. 2025. № 5. Pp. 20–26. (In Russ.) URL: https://cyberleninka.ru/article/n/tendentsii-kiberprestupnosti-analiz-otchetov-o-proisshestviyah-i-uscherbe
12. Senaliev R. B., Risk Assessment and Security Management in Critical Infrastructure Information Systems. R. B. Senaliev, V. G. Yarikov. NBI tekhnologii. [NBI Technologies]. 2024. Vol. 18, № 2. Pp. 40–46. (In Russ.) URL: https://cyberleninka.ru/article/n/otsenka-riskov-i-upravlenie-bezopasnostyu-v-informatsionnyh-sistemah-kriticheskoy-infrastruktury
13. Integration of Cloud, Fog, and Edge Computing: Prospects and Challenges of Digital Transformation. V. A. Cherepenin, I. E. Glazyrin, D. A. Lesnikov, S. P. Vorobyov. Inzhenernyi vestnik Dona. [Engineering Herald of the Don]. 2025. № 2. (In Russ.) URL: https://cyberleninka.ru/article/n/integratsiya-oblachnyh-tumannyh-i-granichnyh-vychisleniy-perspektivy-i-vyzovy-tsifrovoy-transformatsii
14. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection. Guidance on managing information security risks : Publication date 2022-10. Edition 4. 62 p. (In Eng.) URL: https://www.iso.org/standard/80585.html

15. GOST R ISO/IEC 27000-2021. Information technology. Security methods and tools. Information security management systems. General overview and terminology : National Standard of the Russian Federation : official edition : approved and put into effect by Order of the Federal Agency for Technical Regulation and Metrology dated May 19, 2021 No. 392-st : replaces GOST R ISO/IEC 27000-2012 : date of introduction November 30, 2021; prepared by the Federal State Institution “Federal Research Center “Informatics and Control” of the Russian Academy of Sciences, the Limited Liability Company “Information and Analytical Computing Center” and the Joint-Stock Company “Expert” based on their own translation into Russian of the English-language version of the standard specified in paragraph 4. Moscow : Standartinform, 2021. 22 p. (In Russ.)
16. Committee on Information and Legal Security : [official website]. (In Russ.) URL: https://nc-ib.ru/

Статья поступила 17.11.2025
© Н. В. Гуменюк, А. Д. Катунин, 2025
Рецензент: В. Л. Николаенко, канд. техн. наук, доц.,
Автомобильно-дорожный институт
(филиал) ДонНТУ в г. Горловка

Н. В. Гуменюк, А. Д. Катунин

Исследование факторов риска информационной безопасности в телекоммуникационной сфере (на примере телеканала «6ТВ»)

В условиях повсеместной цифровизации и возрастающей зависимости телекоммуникационных компаний от информационных технологий обеспечение информационной безопасности становится критически важным аспектом их функционирования. Телекоммуникационный сектор, включая медиакомпании, относится к числу наиболее уязвимых для кибератак, поскольку сочетает в себе обработку конфиденциальных данных, трансляцию критически важного контента и необходимость обеспечения непрерывности вещания. В связи с этим разработка специализированной модели оценки рисков информационной безопасности является актуальной задачей оптимизации информационной инфраструктуры телеканала и создания проактивной среды для его безопасной работы.

В ходе проведенного исследования проанализированы труды авторитетных ученых, отечественные и международные стандарты в области обеспечения информационной безопасности, которые стали фундаментом разработки гибридной модели управления рисками.

Анализ информационной инфраструктуры телеканала позволил проанализировать статус активов «оборудование», «данные», «программное обеспечение», «персонал», «репутация». Каждому активу был присвоен уровень критичности, влияющий на степень риска, вследствие чего определены важнейшие активы телеканала и соответствующие им угрозы, разработаны критерии классификации активов по уровню важности и степени подверженности угрозам.

В работе выполнен качественный и количественный анализ рисков, в результате чего создана матрица корреляции активов и угроз, отображающая взаимозависимость различных элементов инфраструктуры и конкретных угроз. Доказано, что основными источниками угроз являются устаревшее программное обеспечение и низкая киберграмотность сотрудников. Подтверждена высокая вероятность и тяжесть ряда угроз, таких как взлом CMS «Эфир-ПРО» и утечка архивных записей.

На основе проведенного исследования разработана адаптивная гибридная модель оценки рисков, комбинирующая количественные и качественные методы, на основе которой продемонстрирован алгоритм оценки рисков, позволяющий эффективно оценивать и ранжировать угрозы, описана инструментальная реализация модели с использованием платформ RiskWatch и Tenable.io.

Разработанная модель оценки рисков позволяет повысить уровень защищенности телеканала «6ТВ» до 85 % и сократить операционные риски на 60 %. Использование современных технологий, таких как машинное обучение и блокчейн, обеспечит автоматизацию процессов и проактивное управление угрозами. Модель может быть применена в других регионах с аналогичными вызовами, что подчеркивает ее универсальность и актуальность.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, КИБЕРУГРОЗА, АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, РИСК, ОЦЕНКА УРОВНЯ ЗАЩИЩЕННОСТИ

N. V. Gumeniuk, A. D. Katunin

Research of Information Security Risk Factors in the Telecommunications Sector (Using the Example of the 6TV TV Channel)

In the context of widespread digitalization and the increasing dependence of telecommunications companies on information technology, ensuring information security is becoming a critically important aspect of their functioning. The telecommunications sector, including media companies, is among the most vulnerable to cyber-attacks, as it combines the processing of confidential data, the transmission of critical content and the need to ensure the continuity of broadcasting. In this regard, the development of a specialized information security risk assessment model is an urgent task of optimizing the information infrastructure of the TV channel and creating a proactive environment for its safe operation.

The research analyzed the works of reputable scientists, domestic and international standards in the field of information security, which became the foundation for the development of a hybrid risk management model.

The analysis of the information infrastructure of the TV channel made it possible to analyze the status of assets “equipment”, “data”, “software”, “personnel”, “reputation”. Each asset was assigned a level of criticality that affects the degree of risk, as a result of which the most important assets of the TV channel and their corresponding threats were identified, and criteria for classifying assets by level of importance and degree of threat exposure were developed.

The work performed a qualitative and quantitative risk analysis, resulting in the creation of a matrix of correlation of assets and threats, reflecting the interdependence of various infrastructure elements and specific threats. It isproven that outdated software and low cyber literacy of employees are the main sources of threats. The high probability and severity of a number of threats are confirmed, such as the hacking of the Efir-PRO CMS and the leakage of archived records.

Based on the conducted research, an adaptive hybrid risk assessment model is developed that combines quantitative and qualitative methods, on the basis of which a risk assessment algorithm is demonstrated that makes it possible to effectively assess and rank threats, and an instrumental implementation of the model using RiskWatch platforms and Tenable.io.

The developed risk assessment model makes it possible to increase the security level of the 6TV channel to 85 % and reduce operational risks by 60 %. The use of modern technologies such as machine learning and blockchain will ensure automation of processes and proactive threat management. The model can be applied in other regions with similar challenges, which underlines its versatility and relevance.

INFORMATION SECURITY, INFORMATION INFRASTRUCTURE, CYBER THREAT, INFORMATION SECURITY AUDIT, RISK, SECURITY ASSESSMENT

Сведения об авторах:

Гуменюк Наталья Владимировна
Кандидат экономических наук, доцент,
доцент кафедры «Математическое моделирование» Автомобильно-дорожного института (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Донецкий национальный технический университет» в г. Горловка, ДНР Российская Федерация,
SPIN-код РИНЦ: 8741-7440
ORCID ID: 0000-0002-8076-1955
Телефон: +7 949 412-79-08
Эл. почта: nataligumenuk@rambler.ru

Катунин Александр Дмитриевич
Магистр Автомобильно-дорожного института (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Донецкий национальный технический университет» в г. Горловка, ДНР Российская Федерация,
Телефон: +7 949 467-01-56
Эл. почта: wezert666@mail.ru

Authors' information:

Gumeniuk Natalia Vladimirovna
Candidate of Economic Sciences, Docent,
Associate Professor of the Chair "Mathematical Modelling" of Automobile and Road Institute (Branch) of the Federal State Budget Educational Institution of Higher Education "Donetsk National Technical University" in Gorlovka, DPR, Russian Federation,
RSCI SPIN: 8741-7440
ORCID ID: 0000-0002-8076-1955
Phone: +7 949 412-79-08
Email: nataligumenuk@rambler.ru

Katunin Aleksandr Dmitrievich
Master's Student of Automobile and Road Institute (Branch) of the Federal State Budget Educational Institution of Higher Education "Donetsk National Technical University" in Gorlovka, DPR, Russian Federation,
Phone: +7 949 467-01-56
Email: wezert666@mail.ru