DOI 10.37882/2223-2966.2026.02.19

АУДИТ ЗАЩИЩЕННОСТИ ФИНАНСОВО-КРИТИЧНЫХ ОРГАНИЗАЦИЙ НА ОСНОВЕ OSINT-ТЕХНОЛОГИИ

FINANCIALLY CRITICAL ORGANIZATIONS' SECURITY AUDIT BASED ON OSINT-TECHNOLOGY

V. Kuchmin
I. Krepak

Summary. The article addresses the problem of information security vulnerability auditing in financially critical organizations under conditions of high digital openness and continuous expansion of the external information perimeter. The relevance of using open-source intelligence (OSINT) technology as a tool for preliminary security assessment based on passive analysis of information available from open and legal sources is substantiated. It is shown that the results of OSINT analysis make it possible to identify risk factors formed at the level of the external information environment prior to the implementation of active threats.
The paper proposes a formalized methodology for OSINT-based auditing of the external information perimeter, including a sequence of stages with defined input and output parameters that ensure the reproducibility of analytical results. To demonstrate the practical applicability of the proposed methodology, a conditional example of a financially critical organization is considered, involving qualitative risk factor assessment and interpretation of the obtained data. The limitations and scope of applicability of OSINT auditing within the information security framework are determined. The results obtained can be used in threat modeling, planning information security risk management measures, and improving the maturity of external perimeter protection processes.

Keywords: vulnerability audit, OSINT, financially critical organizations, external information perimeter, risk management, digital footprint, threat model, passive analysis methods, open-source information.

Кучмин Владислав Константинович
ведущий специалист, ФГБОУ ДПО Российская Академия Кадрового Обеспечения Агропромышленный комплекс;
аспирант, Финансовый университет при Правительстве Российской Федерации, г. Москва
severov.14@bk.ru
Крепак Иван Павлович
руководитель группы информационной безопасности, ООО Клиника Будь Здоров;
аспирант, Финансовый университет при Правительстве Российской Федерации, г. Москва
krepak.2311@yandex.ru

Аннотация. В статье рассматривается проблема аудита уязвимостей информационной безопасности финансово-критичных организаций в условиях высокой цифровой открытости и постоянного расширения внешнего информационного периметра. Обосновывается целесообразность использования технологии разведки по открытым источникам (OSINT) в качестве инструмента предварительной оценки защищённости, основанного на пассивном анализе информации, доступной в открытых и легальных источниках. Показано, что результаты OSINT-анализа позволяют выявлять факторы риска, формируемые на уровне внешнего информационного пространства, до реализации активных угроз.
В работе предлагается формализованная методика OSINT-аудита внешнего информационного периметра, включающая последовательность этапов с определёнными входными и выходными параметрами, обеспечивающими воспроизводимость аналитических результатов. Для демонстрации практической применимости методики рассмотрен условный пример финансово-критичной организации с выполнением качественной оценки факторов риска и интерпретацией полученных данных. Определены ограничения и область применимости OSINT-аудита в системе обеспечения информационной безопасности. Полученные результаты могут быть использованы при построении модели угроз, планировании мероприятий по управлению рисками информационной безопасности и повышении зрелости процессов защиты внешнего периметра.

Ключевые слова: аудит уязвимостей, OSINT, финансово-критичные организации, внешний информационный периметр, управление рисками, цифровой след, модель угроз, пассивные методы анализа, открытые источники информации.

Введение

В условиях цифровизации финансово-экономических процессов и активного развития информационных технологий существенно возрастают риски, связанные с нарушением информационной безопасности организаций, осуществляющих обработку персональных и финансово значимых данных. Финансово-критичные организации характеризуются высокой степенью зависимости основных бизнес-процессов от устойчивого функционирования информационных систем, что обусловливает повышенные требования к уровню их защищённости.

Современные финансово-критичные организации активно взаимодействуют с внешней цифровой средой, используя публичные веб-ресурсы, сетевые сервисы, облачные платформы и электронные каналы коммуни-

кации. В результате формируется развитый внешний информационный периметр, значительная часть элементов которого становится доступной для анализа в открытых источниках. Данные сведения могут использоваться как потенциальными нарушителями при подготовке целевых атак, так и специалистами по информационной безопасности в целях выявления факторов риска и повышения уровня защищённости.

В этой связи особую актуальность приобретает использование технологий разведки по открытым источникам (OSINT) в задачах аудита уязвимостей информационной безопасности. В отличие от активных методов оценки защищённости, основанных на тестировании на проникновение, OSINT-подходы позволяют осуществлять анализ внешнего информационного периметра без непосредственного воздействия на информационные системы и без нарушения требований законодательства.

Несмотря на широкое применение OSINT в сфере конкурентной разведки и мониторинга угроз, вопросы его формализованного использования в задачах аудита уязвимостей информационной безопасности финансово-критичных организаций остаются недостаточно разработанными. В большинстве случаев OSINT используется фрагментарно, без чёткой методики и воспроизводимой структуры анализа. Это обусловливает необходимость разработки и обоснования методического подхода к проведению OSINT-аудита как самостоятельного этапа оценки защищённости внешнего периметра.

Целью настоящей статьи является разработка и формализация методики аудита уязвимостей информационной безопасности финансово-критичных организаций на основе технологии OSINT, а также определение области её применимости и ограничений.

Аудит уязвимостей информационной безопасности как подход управления рисками

Аудит уязвимостей информационной безопасности является одной из ключевых процедур в системе управления рисками финансово-критичных организаций. Его основная задача заключается в выявлении потенциальных слабых мест информационной инфраструктуры, которые могут быть использованы для реализации угроз нарушения конфиденциальности, целостности и доступности информации.

В отличие от общего аудита информационной безопасности, ориентированного на проверку соответствия нормативным требованиям и внутренним регламентам, аудит уязвимостей фокусируется на анализе конкретных факторов риска, связанных с архитектурой информационных систем, конфигурацией сетевых сервисов и особенностями эксплуатации цифровых активов. Для финансово-критичных организаций данный вид аудита имеет особое значение [1, 2], поскольку последствия реализации уязвимостей могут приводить к существенным финансовым, правовым и репутационным потерям.

Традиционные подходы к аудиту уязвимостей включают документарный анализ, инструментальный технический аудит, автоматизированное сканирование и тестирование на проникновение. Однако применение активных методов оценки защищённости в финансово-критичных информационных системах часто ограничено организационными и правовыми факторами [3]. Кроме того, указанные методы преимущественно ориентированы на внутренний контур безопасности и не в полной мере учитывают риски, формируемые за пределами контролируемой инфраструктуры [4].

В условиях высокой информационной открытости финансово-критичных организаций существенная часть угроз формируется на уровне внешнего информационного периметра, включающего публичные веб-ресурсы, сетевые сервисы и цифровой след организации в открытых источниках. Анализ данных факторов требует применения методов, ориентированных на пассивный сбор и интерпретацию информации, что обусловливает целесообразность использования технологии OSINT в задачах аудита уязвимостей.

OSINT-технология в задачах обеспечения информационной безопасности финансово-критичных организаций

Технология разведки по открытым источникам представляет собой совокупность методов и инструментов сбора, обработки и анализа информации, находящейся в свободном и легальном доступе. В отличие от закрытых разведывательных и аналитических методов, OSINT основывается исключительно на использовании общедоступных источников информации, что обеспечивает его правовую корректность и возможность применения в деятельности организаций без нарушения требований законодательства [5, 6].

В задачах обеспечения информационной безопасности OSINT используется для анализа внешнего информационного пространства, в котором функционирует организация, а также для выявления и интерпретации её цифрового следа. Под цифровым следом в данном контексте понимается совокупность сведений о доменных ресурсах, сетевой инфраструктуре, используемых технологиях и параметрах конфигурации публичных сервисов, которые могут быть получены из открытых источников без прямого взаимодействия с информационными системами [7, 8].

Для финансово-критичных организаций применение технологии OSINT приобретает особую значимость. Такие организации обрабатывают персональные и финансово значимые данные, а их информационные системы напрямую влияют на устойчивость ключевых бизнес-процессов. При этом, высокая степень цифровой открытости, обусловленная необходимостью публичного взаимодействия с клиентами, партнёрами и государственными структурами, неизбежно приводит к формированию расширенного внешнего информационного периметра. Значительная часть сведений об этом периметре становится доступной в сети Интернет и может использоваться как потенциальными нарушителями, так и специалистами по информационной безопасности.

С методологической точки зрения OSINT в системе обеспечения информационной безопасности целесообразно рассматривать как инструмент предварительного аналитического уровня. Его применение позволяет выявлять потенциальные факторы риска до реализации активных угроз и тем самым дополняет традиционные методы защиты информации. В отличие от средств мониторинга и реагирования, ориентированных на уже произошедшие инциденты, OSINT-подходы направлены на выявление предпосылок возникновения угроз, связанных с избыточной информационной открытостью и архитектурными особенностями внешнего периметра.

Источники OSINT-информации, используемые в задачах информационной безопасности, могут быть условно классифицированы по характеру получаемых данных. К техническим источникам относятся реестры доменных имён, базы данных распределения IP-адресов и автономных систем, а также специализированные поисковые системы сетевых сервисов. Они позволяют получать сведения о сетевой инфраструктуре, доступных протоколах и используемых технологиях. К организационным источникам относятся официальные веб-ресурсы организаций, публикации в государственных реестрах и отчётные материалы, содержащие сведения о структуре и направлениях деятельности. Информационные источники включают средства массовой информации, научные публикации и иные открытые материалы, формирующие контекст функционирования организации в цифровой среде.

Использование указанных источников в совокупности позволяет сформировать целостное представление о внешнем информационном периметре финансово-критичной организации. При этом ключевым преимуществом OSINT является его пассивный характер. Анализ осуществляется на основе уже существующих данных и не предполагает выполнения активных сетевых запросов, сканирования или эксплуатации уязвимостей. Это делает OSINT-подходы особенно актуальными в условиях, когда проведение активных проверок ограничено требованиями регуляторов, внутренними политиками безопасности или необходимостью обеспечения бесперебойной работы информационных систем.

Следует отметить, что в практике обеспечения информационной безопасности технология OSINT часто используется фрагментарно — в виде отдельных инструментов или разрозненных аналитических процедур. Такой подход не позволяет в полной мере реализовать потенциал анализа открытых источников и приводит к снижению воспроизводимости результатов. В этой связи представляется целесообразным рассматривать OSINT не как вспомогательный инструмент, а как основу для формализованного метода аудита уязвимостей внешнего периметра.

Таким образом, технология OSINT занимает промежуточное положение между нормативно-ориентированным аудитом информационной безопасности и активными методами оценки защищённости. Она обеспечивает аналитическую связь между внешним информационным пространством и внутренними механизмами управления информационной безопасностью, позволяя выявлять потенциальные угрозы на ранних этапах и формировать обоснованные управленческие решения. Интеграция OSINT в систему методов обеспечения информационной безопасности финансово-критичных организаций создаёт предпосылки для повышения зрелости процессов управления рисками и снижения вероятности реализации целевых атак.

OSINT-аудит как метод предварительной оценки защищённости внешнего периметра

В современных условиях обеспечения информационной безопасности финансово-критичных организаций особую значимость приобретает необходимость раннего выявления факторов риска, формируемых на уровне внешнего информационного периметра. Традиционные методы оценки защищённости, как правило, ориентированы на анализ внутренних компонентов информационных систем либо предполагают активное воздействие на инфраструктуру объекта исследования. В этой связи целесообразно выделение OSINT-аудита в качестве самостоятельного метода предварительной оценки защищённости, основанного на пассивном анализе открытых источников информации.

Под OSINT-аудитом уязвимостей информационной безопасности предлагается понимать формализованный аналитический процесс выявления и интерпретации факторов риска внешнего информационного периметра организации на основе информации, получаемой из открытых и легальных источников. В отличие от классического аудита информационной безопасности, направленного на проверку соответствия установленным требовани-

ям и регламентам, OSINT-аудит ориентирован на анализ фактической информационной открытости и архитектурных особенностей публичной инфраструктуры.

Ключевой методологической особенностью OSINT-аудита является его предварительный характер. Результаты такого анализа не предназначены для непосредственного выявления эксплуатируемых уязвимостей, а используются для формирования исходных данных при построении модели угроз и определении приоритетных направлений дальнейших защитных мероприятий. Таким образом, OSINT-аудит дополняет существующие методы оценки защищённости, обеспечивая переход от реактивной модели защиты к проактивному управлению рисками.

В отличие от тестирования на проникновение, которое предполагает активное моделирование действий потенциального нарушителя и может сопровождаться рисками нарушения доступности информационных систем, OSINT-аудит не оказывает прямого воздействия на объект исследования [9]. Это делает его особенно актуальным для финансово-критичных организаций, функционирование которых регламентировано строгими требованиями по обеспечению непрерывности бизнес-процессов и соблюдению нормативных ограничений. Кроме того, OSINT-аудит может проводиться на регулярной основе без привлечения значительных ресурсов и без необходимости согласования сложных процедур доступа.

Сравнительный анализ OSINT-аудита и традиционных методов оценки защищённости позволяет определить его место в системе обеспечения информационной безопасности. Если классический аудит ориентирован на внутренние процессы и нормативное соответствие, а тестирование на проникновение — на выявление технических уязвимостей путём активного воздействия, то OSINT-аудит фокусируется на анализе внешнего информационного пространства и факторов риска, связанных с цифровым следом организации. В этом смысле OSINT-аудит следует рассматривать как связующее звено между стратегическим управлением рисками и техническими средствами защиты информации.

С методической точки зрения OSINT-аудит характеризуется высокой воспроизводимостью результатов при условии формализации этапов анализа и критериев оценки. Использование структурированного подхода к сбору и интерпретации данных позволяет минимизировать субъективность выводов и обеспечивает возможность повторного проведения анализа в динамике. Это особенно важно для финансово-критичных организаций, для которых характерны частые изменения внешнего периметра, связанные с развитием цифровых сервисов и интеграцией новых информационных решений.

Следует отметить, что OSINT-аудит не является универсальным методом оценки защищённости и имеет ряд ограничений. Его применение не позволяет выявлять уязвимости, скрытые во внутреннем контуре информационных систем, а также оценивать корректность реализации механизмов аутентификации, авторизации и контроля доступа. Вместе с тем результаты OSINT-аудита обладают высокой практической ценностью на этапе планирования мероприятий по обеспечению информационной безопасности, поскольку позволяют обоснованно определять необходимость и глубину применения активных методов оценки защищённости.

Таким образом, OSINT-аудит уязвимостей информационной безопасности представляет собой самостоятельный метод предварительной оценки защищённости внешнего периметра финансово-критичных организаций, ориентированный на выявление факторов риска и формирование исходных данных для построения модели угроз. Его использование способствует повышению зрелости процессов управления информационной безопасностью и снижению вероятности реализации целевых атак за счёт своевременного выявления потенциально опасных зон внешнего информационного пространства.

Формализация методики OSINT-аудита внешнего периметра

Для обеспечения воспроизводимости результатов и снижения субъективности аналитических выводов OSINT-аудит уязвимостей информационной безопасности должен быть реализован в виде формализованной методики, основанной на последовательном выполнении взаимосвязанных этапов анализа. Формализация методики позволяет рассматривать OSINT-аудит не как совокупность разрозненных действий, а как структурированный процесс, интегрируемый в систему управления информационной безопасностью финансово-критичной организации.

Предлагаемая методика OSINT-аудита ориентирована на анализ внешнего информационного периметра и включает шесть основных этапов, каждый из которых характеризуется определёнными входными данными, методами анализа и выходными результатами [10, 11]. Такая декомпозиция обеспечивает прозрачность процедуры аудита и возможность её повторного применения в динамике.

На первом этапе осуществляется идентификация объекта и границ OSINT-аудита. В качестве входных данных используются общие сведения об организации, включая официальное наименование, используемые доменные зоны и публично декларируемые направления деятельности. Целью данного этапа является опре-

деление границ анализа и формирование первичного перечня цифровых активов, относящихся к внешнему периметру. Результатом этапа является уточнённый список объектов дальнейшего анализа, исключающий нерелевантные или сторонние ресурсы.

Второй этап посвящён анализу доменной структуры внешнего периметра. В рамках данного этапа осуществляется выявление доменных имён и поддоменов, ассоциированных с анализируемой организацией. Входными данными служат результаты предыдущего этапа, а также сведения из открытых доменных реестров и специализированных поисковых инструментов. Выходным результатом является структурированный перечень доменных ресурсов, отражающий степень разветвлённости внешнего периметра и потенциальное расширение поверхности атаки.

На третьем этапе проводится анализ IP-адресного пространства и сетевой принадлежности выявленных ресурсов. В качестве входных данных используются доменные имена, полученные на предыдущем этапе, и информация из открытых баз данных распределения IP-адресов и автономных систем. Целью данного этапа является выявление публичных сетевых диапазонов, используемых организацией, а также определение их принадлежности. Результатом является перечень IP-адресов и сетевых диапазонов, формирующих сетевую составляющую внешнего периметра.

Четвёртый этап ориентирован на анализ доступных сетевых сервисов и используемых протоколов. Входными данными служат IP-адреса и доменные ресурсы, полученные на предыдущих этапах. На данном этапе выявляются публично доступные сервисы, их назначение и базовые параметры конфигурации. Результаты этапа позволяют оценить уровень экспонирования инфраструктурных компонентов и определить потенциально уязвимые зоны внешнего периметра [13, 14].

Пятый этап включает анализ параметров защиты публичных сервисов, в том числе характеристик защищённых соединений и используемых криптографических механизмов. В качестве входных данных используются сведения о сетевых сервисах и протоколах, а также информация, доступная в открытых источниках о параметрах TLS/SSL-соединений. Выходными результатами этапа являются качественные характеристики применяемых механизмов защиты, позволяющие судить об уровне базовой криптографической устойчивости внешнего периметра.

Заключительный этап методики направлен на обобщение и интерпретацию полученных результатов. На данном этапе осуществляется систематизация данных, выявленных на предыдущих стадиях, и формирование аналитических выводов. Результаты OSINT-аудита используются для предварительной классификации факторов риска, уточнения модели угроз и определения приоритетов дальнейших мероприятий по обеспечению информационной безопасности [12]. Итогом этапа является аналитический отчёт, содержащий обобщённую оценку состояния внешнего периметра и рекомендации по дальнейшему анализу.

Следует отметить, что формализация этапов OSINT-аудита обеспечивает возможность адаптации методики под специфику конкретной финансово-критичной организации. В зависимости от масштаба инфраструктуры, уровня цифровой открытости и регуляторных требований отдельные этапы могут быть детализированы или агрегированы без нарушения общей логики анализа. Это делает предложенную методику универсальным инструментом предварительной оценки защищённости внешнего информационного периметра.

Пример применения методики OSINT-аудита

Для демонстрации практической применимости разработанной методики OSINT-аудита рассмотрим условную финансово-критичную организацию, осуществляющую обработку персональных и финансовых данных и использующую публичные цифровые ресурсы для взаимодействия с внешними пользователями. В рамках примера предполагается, что анализ проводится исключительно на основе информации, доступной в открытых источниках, без активного воздействия на информационные системы.

В качестве исходных данных для OSINT-аудита внешнего периметра примем следующие параметры, характеризующие уровень информационной открытости условной организации.

Таблица 1.

Входные данные условного примера OSINT-аудита

Параметр	Обозначение	Значение
Количество доменных ресурсов	D	12
Количество поддоменов	D_s	27
Количество публичных IP-диапазонов	I	3
Количество доступных сетевых сервисов	S	8
Критичность обрабатываемых данных	C	Высокая

Обозначенные параметры отражают типичную структуру внешнего периметра финансово-критичной организации со средним уровнем цифровой зрелости и развитой сетевой инфраструктурой. Наличие нескольких доменных ресурсов и поддоменов указывает на расширенную поверхность атаки, а присутствие публичных

сервисов — на потенциальную доступность инфраструктурных компонентов для внешнего анализа.

Для формализации оценки потенциальных рисков используется логическая модель следующего вида:

$$R = f(D, D_s, S, I, C)$$

Где: R — интегральный уровень риска внешнего периметра,
D — количество доменных ресурсов,
D_s — количество поддоменов,
S — количество публичных сетевых сервисов,
I — количество сетевых диапазонов,
C — критичность обрабатываемых данных.

В рамках качественного анализа параметры D, D_s, S и I рассматриваются как факторы, определяющие вероятность реализации угроз, связанных с внешним периметром, тогда как параметр C характеризует потенциальный масштаб ущерба при успешной реализации угрозы. Увеличение значений параметров D и D_s приводит к росту сложности контроля внешнего периметра и повышает вероятность наличия неконтролируемых точек входа. Рост параметра S отражает расширение набора доступных сервисов и, соответственно, увеличение потенциальных векторов атак.

На основе предложенной модели выполняется качественная классификация факторов риска, полученных в результате OSINT-аудита.

Таблица 2.

Классификация факторов риска внешнего периметра

Фактор	Характеристика	Влияние на риск
Доменная структура	Разветвлённая система доменов и поддоменов	Повышает
Сетевые сервисы	Наличие инфраструктурных и прикладных сервисов	Повышает
IP-адресное пространство	Несколько публичных диапазонов	Умеренное
Критичность данных	Финансовые и персональные данные	Существенное

Интерпретация полученных результатов позволяет сделать вывод о наличии повышенного уровня потенциальных рисков, связанных с внешним информационным периметром условной финансово-критичной организации [15]. В частности, выявленная разветвлённая доменная структура и наличие публичных сервисов требуют повышенного внимания при построении модели угроз и выборе мер защиты.

Таким образом, применение разработанной методики OSINT-аудита позволяет на основе формализованных входных данных выполнить предварительную оценку состояния защищённости внешнего периметра, определить приоритетные направления дальнейшего анализа и обосновать необходимость применения более детализированных методов оценки защищённости, включая активные проверки.

Ограничения и область применимости метода OSINT-аудита

Несмотря на широкие аналитические возможности, метод OSINT-аудита уязвимостей информационной безопасности обладает рядом объективных ограничений, обусловленных спецификой используемых источников данных и пассивным характером анализа [16]. Осознание данных ограничений является необходимым условием корректной интерпретации результатов и повышения практической ценности применения метода в системе обеспечения информационной безопасности финансово-критичных организаций.

Прежде всего, OSINT-аудит ориентирован исключительно на анализ информации, находящейся в открытых и легальных источниках, и не позволяет выявлять уязвимости, связанные с внутренними компонентами информационных систем, включая конфигурации серверов, механизмы аутентификации и авторизации, а также процессы управления доступом. В этой связи результаты OSINT-аудита следует рассматривать как предварительную оценку состояния защищённости внешнего периметра, а не как исчерпывающий анализ всех аспектов информационной безопасности организации.

Ограничения метода также связаны с возможной неполнотой и актуальностью данных, доступных в открытых источниках. Информация о доменных ресурсах, сетевых сервисах и параметрах конфигурации может обновляться с различной периодичностью, что требует регулярного повторения OSINT-аудита для поддержания актуальности аналитических выводов. При этом сама методика допускает повторное применение без значительных ресурсных затрат, что частично компенсирует указанный недостаток.

Следует отметить, что OSINT-аудит не предназначен для выявления факта эксплуатации уязвимостей и не позволяет оценить устойчивость информационных систем к целенаправленным атакам. Его применение не заменяет активные методы оценки защищённости, такие как тестирование на проникновение и технический аудит, а дополняет их, формируя исходную аналитическую базу для принятия управленческих решений в области информационной безопасности.

Областью наибольшей применимости метода OSINT-аудита являются финансово-критичные организации

с развитой публичной сетевой инфраструктурой и высокой степенью информационной открытости. Метод особенно эффективен на этапах инвентаризации цифровых активов, построения модели угроз и определения приоритетов дальнейших защитных мероприятий. В условиях строгих регуляторных требований и ограничений на проведение активных проверок OSINT-аудит может использоваться в качестве регулярного инструмента мониторинга состояния внешнего информационного периметра.

Таким образом, метод OSINT-аудита целесообразно рассматривать как компонент комплексной системы оценки защищённости, обеспечивающий предварительный анализ факторов риска и повышающий эффективность применения более детализированных методов обеспечения информационной безопасности. Корректное понимание ограничений и области применимости метода позволяет интегрировать его в процессы управления рисками без снижения достоверности итоговых выводов.

Заключение

В результате проведённого исследования разработан и обоснован методический подход к аудиту уязвимостей информационной безопасности финансово-критичных организаций на основе технологии OSINT. В отличие от традиционных методов оценки защищённости, ориентированных на внутренний контур информационных систем или активное воздействие на инфраструктуру, предложенный подход направлен на анализ внешнего информационного периметра и факторов риска, формируемых в открытом информационном пространстве.

В рамках исследования сформулировано авторское определение OSINT-аудита как метода предварительной оценки защищённости, основанного на пассивном анализе открытых источников информации. Предложенная формализованная методика OSINT-аудита включает последовательность взаимосвязанных этапов, обеспечивающих воспроизводимость аналитических результатов и снижение субъективности при интерпретации полученных данных. Декомпозиция процесса аудита на этапы с определёнными входными и выходными параметрами позволяет интегрировать метод в систему управления информационной безопасностью финансово-критичных организаций.

Для демонстрации практической применимости методики рассмотрен условный пример анализа внешнего периметра финансово-критичной организации. Использование формализованных входных данных и логической модели оценки рисков позволило выполнить качественную классификацию факторов риска и обосновать необходимость применения дополнительных мер защиты. Полученные результаты подтверждают возможность использования OSINT-аудита в качестве самостоятельного аналитического инструмента на этапе построения модели угроз и планирования мероприятий по обеспечению информационной безопасности.

Показано, что OSINT-аудит обладает рядом объективных ограничений, обусловленных пассивным характером анализа и зависимостью от полноты данных, доступных в открытых источниках. Вместе с тем его применение позволяет существенно повысить эффективность процессов управления рисками за счёт раннего выявления потенциально опасных зон внешнего информационного периметра и обоснованного определения приоритетов дальнейших защитных мероприятий.

Практическая значимость результатов исследования заключается в возможности использования разработанной методики OSINT-аудита в деятельности подразделений информационной безопасности финансово-критичных организаций в качестве инструмента предварительного анализа и мониторинга состояния внешнего периметра. Перспективы дальнейших исследований связаны с апробацией методики на реальных объектах и расширением модели оценки рисков с использованием количественных показателей и автоматизированных средств анализа.

ЛИТЕРАТУРА

1. Аверченков В.И. Аудит информационной безопасности: учеб. пособие. — М.: Горячая линия — Телеком, 2020. — 240 с.
2. Баранов А.П., Королев И.Д. Управление рисками информационной безопасности в финансовых организациях // Финансовая безопасность. — 2022. — № 2. — С. 45–52.
3. Банк России. Основные направления развития информационной безопасности в кредитно-финансовой сфере. — М., 2022. — 36 с.
4. Попова О.С., Попов А.А., Дровникова И.Г. Развитие интеллектуальных технологий в SIEM-системах // Безопасность информационных технологий. — 2023. — № 4. — С. 18–27.
5. Ющук Е.Л. Конкурентная разведка. Маркетинг рисков и возможностей. — М.: Вершина, 2019. — 384 с.
6. Steele R. D. The New Craft of Intelligence. — Oakton: Open-Source Solutions, 2012. — 320 p.
7. Bazzell M. Open-Source Intelligence Techniques. — 9th ed. — Intel Techniques, 2023. — 620 p.
8. Casey E. Digital Evidence and Computer Crime. — 4th ed. — Amsterdam: Academic Press, 2019. — 800 p.
9. Behl A., Behl K. Cybersecurity and Cyberwar: What Everyone Needs to Know. — Oxford: Oxford University Press, 2017. — 296 p.

10. ISO/IEC 27001:2022. Information security management systems — Requirements.
11. ISO/IEC 27005:2018. Information security risk management.
12. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems. — Gaithersburg: NIST, 2018.
13. NIST SP 800-61 Rev.2. Computer Security Incident Handling Guide. — Gaithersburg: NIST, 2018.
14. NIST SP 800-30 Rev.1. Guide for Conducting Risk Assessments. — Gaithersburg: NIST, 2019.
15. ENISA. Threat Landscape Report. — Heraklion: European Union Agency for Cybersecurity, 2023.
16. Choo K.-K.R. Cybercrime and cybersecurity: Challenges and opportunities // Journal of Information Security. — 2020. — Vol. 11. — P. 1–9.