Петлеванный Алексей Александрович
Краснодарское высшее военное училище
имени генерала армии С. М. Штеменко
Petlevanny Alexey Alexandrovich

Рожков Виталий Григорьевич
Краснодарское высшее военное училище
имени генерала армии С. М. Штеменко
Rozhkov Vitaly Grigorievich

Зимин Дмитрий Юрьевич
Краснодарское высшее военное училище
имени генерала армии С. М. Штеменко
Zimin Dmitry Yurievich

Ничунаев Артем Александрович
Краснодарское высшее военное училище
имени генерала армии С. М. Штеменко
Nichunaev Artem Alexandrovich

КЛАССИФИКАЦИЯ ВОЗМОЖНЫХ ТРЕБОВАНИЙ К ПЕРСПЕКТИВНЫМ СРЕДСТВАМ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ
CLASSIFICATION OF POSSIBLE REQUIREMENTS FOR ADVANCED MEANS OF INFORMATION PROTECTION AGAINST LEAKAGE VIA TECHNICAL CHANNELS

Аннотация. Статья рассматривает классификацию требований к перспективным средствам защиты информации от утечки по техническим каналам. Выделяются функциональные, технические, эксплуатационные и организационно-правовые аспекты, необходимые для эффективного противодействия угрозам информационной безопасности. Предлагаются направления развития, включающие использование методов искусственного интеллекта, разработку адаптивных систем и повышение устойчивости к комбинированным угрозам

Abstract. The article discusses the classification of requirements for advanced information protection systems against leakage through technical channels. Functional, technical, operational, and organizational-legal aspects necessary for effective countering of information security threats are highlighted. Development directions are proposed, including the use of artificial intelligence methods, development of adaptive systems, and increased resilience to combined threats

Ключевые слова: Информационная безопасность, технические каналы утечки, классификация требований, перспективы развития, средства защиты информации, мониторинг утечек, методы искусственного интеллекта, побочные каналы утечки, криптографическая защита, нормативные стандарты

Keywords: Information security, technical leakage channels, classification of requirements, development prospects, information protection means, leakage monitoring, artificial intelligence methods, side channels of information leakage, cryptographic protection, regulatory standards

Современный этап развития цифровых и автоматизированных систем характеризуется ростом объёмов обрабатываемой информации и усложнением угроз информационной безопасности. Наряду с программными и сетевыми атаками особую опасность представляют утечки информации по техническим каналам, реализуемые без непосредственного логического доступа к данным.

Анализ угроз информационной безопасности автоматизированных систем показывает, что технические каналы утечки информации отличаются высокой скрытностью и трудоёмкостью обнаружения [2]. Развитие высокочувствительных средств регистрации и цифровой обработки сигналов существенно расширяет возможности несанкционированного съёма информации.

Дополнительным фактором актуализации проблемы является развитие доктрин информационного воздействия и киберпротивоборства, в которых техническая разведка рассматривается как важный элемент достижения информационного превосходства [3]. В этих условиях возрастает роль перспективных средств защиты информации, способных противостоять утечкам по техническим каналам на основе заранее сформулированных и научно обоснованных требований.

Технические каналы утечки информации формируются в результате преобразования информативных сигналов в физические поля и излучения, сопровождающие работу технических средств обработки, хранения и передачи информации. К таким каналам относятся электромагнитные, акустические, виброакустические, оптические и параметрические каналы.

Современные исследования побочных каналов утечки информации показывают, что наибольшую опасность представляют комбинированные каналы, в которых информация проявляется одновременно в нескольких физических формах [5]. Это существенно усложняет задачи обнаружения и подавления утечки и требует применения комплексных средств защиты.

Практика разработки сложных технических систем обнаружения и локализации источников физических процессов, в том числе в смежных областях измерений и мониторинга, показывает эффективность методов пространственно-временной обработки сигналов и адаптивного анализа [1]. Указанные подходы могут быть применены и в средствах защиты информации от утечки по техническим каналам.

Анализ угроз информационной безопасности автоматизированных систем показывает, что технические каналы утечки информации остаются устойчивым и трудно контролируемым классом угроз [2]. Их реализация возможна даже при наличии развитых средств криптографической и программной защиты.

Зарубежные исследования подтверждают активное развитие атак по побочным каналам, включая энергетические, временные и электромагнитные каналы утечки [4, 5]. В условиях реализации доктрин информационного воздействия такие каналы могут использоваться для скрытого получения конфиденциальной информации и подготовки последующих воздействий [3].

Указанные факторы формируют необходимость разработки перспективных средств защиты информации, ориентированных на адаптивность, интеллектуальность и комплексность, что требует систематизации требований к таким средствам.

Классификация требований к перспективным средствам защиты информации представлена на рисунке 1, показывающий взаимосвязи между группами требований и их функциональными задачами.

Рисунок 1 - Схема классификации требований
к перспективным средствам защиты информации

К функциональным требованиям относятся требования, определяющие основные задачи средств защиты информации:

- обнаружение фактов формирования технических каналов утечки;
- идентификация типа и физической природы канала утечки;
- оценка уровня информативности утечки;
- локализация источников утечки;
- активное или пассивное подавление каналов утечки;
- регистрация и анализ инцидентов информационной безопасности.

Современные исследования подчёркивают необходимость интеграции функций мониторинга, анализа и противодействия в рамках единого защитного комплекса [4, 6].

Технические требования определяют количественные и качественные характеристики средств защиты информации:

- высокая чувствительность средств обнаружения;
- устойчивость к внешним и преднамеренным помехам;
- возможность работы в широком диапазоне частот и уровней сигналов;
- точность временной и пространственной локализации источников утечки;
- совместимость с существующими инженерно-техническими системами объекта.

Как показывают современные исследования в области оценки побочных каналов утечки, повышение точности и устойчивости средств защиты напрямую влияет на эффективность противодействия утечкам информации [5].

Эксплуатационные требования связаны с практическим применением средств защиты информации:

- высокая надёжность и отказоустойчивость;
- возможность длительной непрерывной эксплуатации;

- минимальные требования к техническому обслуживанию;
- простота настройки и эксплуатации;
- адаптация к изменяющимся условиям функционирования.

Использование интеллектуальных методов анализа сигналов позволяет снизить нагрузку на обслуживающий персонал и повысить эффективность эксплуатации средств защиты [6].

Организационно-правовые требования определяются действующей нормативной базой и условиями применения средств защиты информации и включают:

- соответствие требованиям стандартов и методических документов;
- возможность сертификации средств защиты;
- совместимость с режимами ограничения доступа к информации;
- обеспечение юридической значимости результатов контроля.

Особую значимость данные требования приобретают в условиях применения средств защиты информации на критически важных объектах и в системах государственного управления [3].

Для наглядного представления требований составлена таблица 1, где приведены группы требований, их содержание и примеры реализации. Данная таблица иллюстрирует структурированное представление требований к перспективным средствам защиты информации от утечки по техническим каналам.

Таблица 1

Табличная систематизация требований

Группа требований	Содержание	Пример реализации
Функциональные	Блокирование ТКУИ	Экранирование, активное подавление
Технические	Параметры защиты	Ослабление ≥ 60 дБ, диапазон частот 0,1–100 МГц
Эксплуатационные	Надёжность	Наработка на отказ, ремонтопригодность
Аналитические	Контроль эффективности	Системы мониторинга, адаптивная настройка
Организационные	Соответствие стандартам	Сертификация СЗИ, соответствие ГОСТ

Перспективные направления развития требований.

Работы по военно-технической доктрине показывают, что утечки через технические каналы могут использоваться для скрытого получения конфиденциальной информации, что требует высокой адаптивности и интеллектуальности СЗИ [3].

Анализ современных тенденций позволяет выделить следующие направления развития требований к перспективным средствам защиты информации:

- применение методов машинного обучения и искусственного интеллекта;
- развитие адаптивных и самообучающихся систем защиты [7-8];
- интеграция средств защиты в комплексные системы мониторинга;
- повышение скрытности функционирования средств защиты;
- обеспечение устойчивости к гибридным и комбинированным угрозам.

Данные направления подтверждаются результатами современных исследований побочных каналов утечки информации и методов противодействия им [4-6].

Предлагаемая классификация требований к перспективным средствам защиты информации от утечки по техническим каналам отражает комплексный характер современной информационной безопасности. Эффективная система защиты должна включать разнообразные методы противодействия угрозам, объединяя организационные мероприятия, технологические решения и правовые инструменты. Одним из важнейших факторов успеха является автоматизация процессов мониторинга и анализа информации, позволяющая быстро

обнаруживать подозрительные активности и предотвращать утечку данных. Инновационные подходы, такие как применение искусственного интеллекта и машинного обучения, позволяют разрабатывать умные системы, автоматически распознающие признаки атак и предупреждающие нарушения безопасности. Большое значение также имеет подготовка квалифицированных специалистов, способных грамотно управлять системами защиты и своевременно реагировать на возникающую угрозу. Наконец, постоянная модернизация нормативной базы играет ключевую роль в адаптации предприятий к новым видам угроз и обеспечении соответствия актуальным стандартам безопасности. Все перечисленные факторы формируют единую систему защиты, направленную на снижение риска утечек информации и обеспечение надежного функционирования инфраструктуры организации в цифровом пространстве

Список литературы:

1. Патент № 2730420 C1 Российская Федерация, МПК F41J 5/00, G01V 1/24, G01V 1/30. Способ определения координат места падения боеприпаса: № 2020106341: заявл. 10.02.2020: опубл. 21.08.2020 / А. В. Акишин, А. Е. Смелов, С. А. Иванов [и др.]. – EDN KLLLMM.

2. Охотин Д. А., Акишин А. В., Хечиев Н. В [и др.] Анализ и классификация угроз информационной безопасности на автоматизированных системах // Вектор научной мысли. – 2025. – № 1 (18). – С. 389-392. – EDN OCDJJU.

3. Алашеев В. В., Акишин А. В., Чеснаков М. Н. Взгляды США на разработку доктрины информационного воздействия в киберпространстве // Проблемы технического обеспечения войск в современных условиях. – СПб., 2018. – Т. 1. – С. 67-71. – EDN XMGZPF.

4. Sanjaya S., Jayasena A., Mishra P. Application-Specific Power Side-Channel Attacks and Countermeasures: A Survey // arXiv. – 2025.

5. Wang Y., Tang M. A Survey of Side-Channel Leakage Assessment // Electronics. – 2023. – Vol. 12, № 16.

6. Mahfuz T., Paria S., Bhunia S., Chakraborty P. POLARIS: Explainable Artificial Intelligence for Mitigating Power Side-Channel Leakage // arXiv. – 2025.

7. Ковалёв И. А., Смирнов П. Н. Технические каналы утечки информации в автоматизированных системах // Информационная безопасность. – 2022. – № 4. – С. 15-22.

8. Белов А. С., Фёдоров М. В. Перспективные средства защиты информации от побочных электромагнитных излучений // Защита информации. Инсайд. – 2023. – № 6. – С. 28-35.

9. Сидоров К. Л. Интеллектуальные системы мониторинга утечек информации по техническим каналам // Вопросы кибербезопасности. – 2024. – № 2. – С. 41-48