Интернет-журнал «Отходы и ресурсы» https://resources.today
Russian Journal of Resources, Conservation and Recycling

2025, Том 12, № 2 / 2025, Vol. 12, Iss. 2 https://resources.today/issue-2-2025.html

URL статьи: https://resources.today/PDF/01NZOR225.pdf

DOI: 10.15862/01NZOR225 (https://doi.org/10.15862/01NZOR225)

2.3.1. Системный анализ, управление и обработка информации, статистика (технические науки)

Ссылка для цитирования этой статьи:
Чабанов, И. Д. Анализ и разработка моделей для обнаружения технических каналов утечки информации с применением машинного обучения / И. Д. Чабанов // Отходы и ресурсы. — 2025. — Т. 12. — № 2. — URL: https://resources.today/PDF/01NZOR225.pdf. DOI: 10.15862/01NZOR225.

For citation:
Chabanov I.D. Analysis and development of models for detection of technical information leakage channels using machine learning. *Russian Journal of Resources, Conservation and Recycling*. 2025;12(2): 01NZOR225. Available at: https://resources.today/PDF/01NZOR225.pdf. DOI: 10.15862/01NZOR225. (In Russ., abstract in Eng.).

УДК 004.942

Чабанов Илья Дмитриевич
ФГАОУ ВО «Дальневосточный федеральный университет», Владивосток, Россия
Старший преподаватель
E-mail: Chabanov.id@dvfu.ru; slepoivareskyn@gmail.com
РИНЦ: https://elibrary.ru/author_profile.asp?id=1291373

Анализ и разработка моделей для обнаружения технических каналов утечки информации с применением машинного обучения

Аннотация. В статье рассматривается проблема обнаружения технических каналов утечки информации в условиях роста сложности и изощренности современных угроз информационной безопасности. Актуальность исследования обусловлена необходимостью автоматизации процессов поиска скрытых устройств, что особенно важно для организаций малого и среднего бизнеса, которые не могут позволить себе дорогостоящее оборудование и высококвалифицированных специалистов.

Авторы анализируют существующие методы обнаружения утечек, включая радиомониторинг, анализ электромагнитных полей и проверку токоведущих линий, и выделяют их ключевые ограничения: зависимость от экспертов, высокую стоимость и недостаточную адаптивность к скрытым угрозам. В качестве решения предлагается применение методов машинного обучения, способных анализировать аномалии в радиочастотных сигналах без прямого участия человека.

В работе детально рассмотрены четыре модели классификации, каждая из которых фокусируется на разных параметрах сигналов: соответствие частот легитимным устройствам; временные паттерны активности; периодичность появления сигналов; локализация источников излучения.

Научная новизна исследования заключается в разработке гибридной системы, объединяющей эти модели с использованием метода взвешенного голосования. Такой подход позволяет минимизировать ложные срабатывания и повысить точность детектирования. Практическая значимость работы заключается в создании экономически эффективного решения, совместимого с существующими системами защиты информации.

Перспективы дальнейших исследований включают расширение набора анализируемых признаков, тестирование в реальных условиях и внедрение в реальные практики организации информационной безопасности на предприятиях.

Ключевые слова: технические каналы утечки информации; машинное обучение; радиочастотный анализ; защита информации; автоматизация мониторинга; гибридная модель; аномалии сигналов

Введение

Современные угрозы информационной безопасности становятся все более изощренными. Ручные методы поиска технических каналов утечки информации, такие как визуальный осмотр и использование простых детекторов, зачастую оказываются недостаточно эффективными. Злоумышленники могут внедрять скрытые устройства в предметы быта, что усложняет их обнаружение без специализированного оборудования. Наличие техники, содержащей закладное устройство, обусловлено высоким ростом популярности IoT систем и возможностью заказа IoT устройств и бытовой техники с различных маркетплейсов, в том числе и зарубежных.

Обнаружение и предотвращение утечек информации требует высокой квалификации специалистов. Необходимы глубокие знания в области электроники, информационных технологий и методов защиты информации. В условиях быстрого развития технологий поддержание высокого уровня экспертизы становится сложной задачей, требующей постоянного обучения и повышения квалификации.

Современные технологии и оборудование для обнаружения технических каналов утечки информации являются дорогостоящими. Они в себя включают различного рода детекторы скрытых микрофонов и видеокамер, индикаторы электромагнитных полей, радиочастотомеры и автоматизированные программно-аппаратные комплексы. Высокая стоимость такого оборудования ограничивает его доступность для многих организаций, особенно малого и среднего бизнеса, не говоря уже об использовании в домашних условиях.

Еще одним фактором, указывающим на актуальность технических каналов утечки информации, это строгие регламенты Федеральной службы по техническому и экспортному контролю России в области технической защиты информации. В условиях постоянного роста числа и сложности киберугроз, защита данных становится приоритетной задачей для любого предприятия и государственного учреждения.

Регламенты ФСТЭК устанавливают высокие стандарты безопасности, требуя применения передовых технологий и методов для предотвращения утечек информации через технические каналы. Эти требования подчеркивают необходимость использования автоматизированных систем, способных эффективно обнаруживать скрытые угрозы и предотвращать несанкционированный доступ к конфиденциальным данным.

Модели машинного обучения могут значительно упростить процесс выявления скрытых угроз. Они способны анализировать большие объемы данных, выявлять аномалии и с высокой точностью определять нелегитимные источники сигналов.

Данное решение снижает зависимость от человеческого фактора и повышает общую эффективность систем защиты информации. Применение моделей позволяет не только соответствовать нормативным требованиям, но и повышать общий уровень защиты информации, что особенно важно в условиях цифровизации и глобализации.

Методы обнаружения технических каналов утечки информации

В общем случае весь процесс выявления устройств негласного съема информации можно представить в виде последовательности следующих этапов [1]:

- Этап подготовки.
- Визуальный осмотр и физический поиск.
- Выявление закладных устройств с передачей информации по радиоканалу.
- Выявление закладных устройств с передачей информации по токоведущим линиям.
- Выявление закладных устройств с передачей информации по ИК-каналу.
- Выявление акустических и виброакустических каналов утечки информации.[1]

Перечисленные выше этапы проведения поисковых мероприятий можно реализовать с помощью различных методов поиска устройств негласного съема информации.

Тестирование телефонных аппаратов включает в себя проверку телефонных линий путем посылки сигналов с автоматической телефонной станции. Данный метод направлен на выявление возможных утечек информации через телефонные линии, которые могут быть использованы злоумышленниками для перехвата разговоров. Сигналы отправляются по телефонной линии, после чего анализируются любые отклонения или аномалии в ответных сигналах.

Анализ распространения сигналов в каналах связи охватывает проверку различных типов связи на предмет возможных утечек информации. Данный метод включает в себя мониторинг и анализ сигналов в различных частотных диапазонах, а также проверку на наличие несанкционированных подключений с целью обнаружения несанкционированного распространения данных через различные каналы связи.

Следующий метод основан на использование индикаторов электромагнитных полей. Эти устройства регистрируют превышение фонового уровня напряженности электромагнитного излучения. Индикаторы размещаются в предполагаемых местах установки закладных устройств, и при превышении порогового уровня излучения подается сигнал тревоги. Таким образом возможно обнаружить закладные устройства, которые могут излучать электромагнитные сигналы.

Для выявления несанкционированных радиопередатчиков и радиозакладок используются радиочастотометры и средства сканирования радиосигналов. Радиочастотометры сканируют радиочастотный спектр и выявление сигналов, превышающие пороговые значения. Анализаторы спектра автоматически сканируют широкий диапазон радиочастот и анализируют сигналы на наличие аномалий.

Радиомониториг является одним из наиболее эффективных и часто используемых методов обнаружения технических каналов утечки информации. Особенности использования средств для мониторинга радиочастот:

Широкий охват частот. Радиомониторинг позволяет сканировать широкий диапазон радиочастот, что делает данный метод универсальным инструментом для выявления различных типов несанкционированных радиосигналов.

[1] Горбачев А.А. Техническая защита информации. Поисковые приборы: учебное пособие / А.А. Горбачев, С.И. Алешников. — Калининград: Издательство БФУ им. Канта, 2022. — 148 с., ISBN 978-5-9971-0696-6.

Высокая чувствительность. Современные сканирующие приемники и анализаторы спектра обладают высокой чувствительностью, что позволяет обнаруживать даже слабые сигналы, которые могут быть незаметны другими методами. Данный аспект особенно важен при выявлении скрытых радиозакладных устройств.

Автоматизация процессов. Системы радиомониторинга могут представлять готовый комплекс, способный автоматически проводить анализ радиочастотного диапазона и классифицировать сигналы. Это значительно ускоряет процесс поиска и анализ подозрительных сигналов, снижая вероятность пропуска угроз.

Системы радиомониторинга сами по себе не могут определить является ли частота каналом утечки информации или же легитимной активностью. Различные исследования в данной области показывают, что при помощи средств радиомониторинга можно реализовать механизм быстрого сканирования, который позволит визуально построить разностную картину между различными измерениями радиочастотного сигнала, но результат работы данного механизма выделит частотные участки, к которым можно применить дальнейшие мероприятия по анализу и распознаванию сигналов, но данные измерения не гарантируют, что выделенные частоты будут являться следствием работы радиозакладных устройств [2].

Использование существующих инструментов и методов эффективно при наличии эксперта в данной области, что в свою очередь создает проблему для поиска технических каналов утечки для представителей малого и среднего бизнеса. Необходимость наличия эксперта при поиске устройств негласного съема информации влечет за собой несколько проблем — требования к квалификации специалиста, проводящего поисковые мероприятия и дороговизна мероприятий.

Использование методов машинного обучения может решить данную проблему и увеличит уровень информационной безопасности. В настоящее время существует реализация нейронной сети для поиска технических каналов утечки информации. Данная нейронная сеть выполняет задачу по поиску технических каналов утечки информации, но допускает ошибки, что объясняется недостаточным количеством признаков [3].

В силу того, что нейронные сети являются подклассом машинного обучения, следует рассмотреть возможность применения методов машинного обучения для обнаружения подобных утечек. Целью данной работы является анализ возможности применения методов машинного обучения для решения задачи по поиску технических каналов утечки информации без использования высококвалифицированного специалиста [4–10].

Модели машинного обучения для поиска технических каналов утечки информации

В результате работы модели необходимо получить прогноз является ли излучение на определенной частоте работой устройства негласного съема информации или же это штатная работа аппаратуры внутри рассматриваемого контура. Для решения задачи определения технического канала утечки информации предлагается использовать модели классификации.

На модель подаются данные, которые содержат в себе следующую информацию: частота, интенсивность сигнала, координаты приемника, время активности. Для сбора данной информации предлагается установить приемник в контролируемой зоне, который эти данные будет собирать. Рассмотрим модели, которые мы можем построить на основе этих данных.

Модель 1. У эксперта имеется перечень легитимных устройств, которые работают в рамках рассматриваемого помещения и могут создавать радиочастотное излучение. Таким образом возможно узнать конкретные частоты, которые можно отнести к санкционированной работе устройств, следовательно модель будет работать по следующему правилу: если частота

излучения не равняется ни одному значению из списка легитимных частот, то такая частота будет нелегитимной. Результат обработки данных с выводом «нелегитимная» будет сигнализировать специалистам по защите информации о необходимости проверки данного частотного диапазона.

Проблема модели заключается в том, что некоторые устройства для негласного съема информации могут работать в легитимном радиочастотном диапазоне. Чем выше уровень квалификации злоумышленника, тем с большей вероятностью устройство будет обладать возможностью маскироваться. Помимо этого, существует проблема сбора легитимных частот, в некоторую аппаратуру уже могут быть встроенные закладки, которые будут создавать определенное излучение при запуске штатного оборудования, следовательно такое излучение при построении эталонного спектра будет расцениваться как легитимное.

Модель 2. Все излучение в контролируемом помещении вызваны стандартной работой технических средств: персональный компьютер, принтер, монитор, факс и т. д. В таком случае понятно, что данное оборудование активно только в рабочее время, непосредственно при взаимодействии пользователя с данными устройствами. Исходя из этого можем сформировать следующее правило: если излучение зафиксировано в период 18:00–07:00 местного времени или излучение зафиксировано в субботу или воскресенье, то оно считается нелегитимным.

Данная модель уже сможет работать в тех случаях, если сигнал может маскироваться под легитимный, но при этом имеет свои недостатки. Сотрудники зачастую могут оставаться после работы для того, чтобы закончить выполнение срочных задач. Кто-то может дистанционно взаимодействовать с устройствами, используя протоколы удаленного управления.

Модель 3. Устройства негласного съема информации могут иметь разный принцип работы. Существуют устройства, который в течение какого-то периода времени могу только слушать, собирать информацию и хранить внутри себя, пока память устройства не заполнится. После этого устройство должно выйти в эфир и передать накопившуюся информацию злоумышленнику. Для детектирования работы подобных устройств модель должна работать по следующему правилу: если данная частота была неактивна в течение 30 предыдущих дней, то можем считать излучение на данной частоте нелегитимным.

Модель решает вопрос с устройствами, которые работают не на постоянной основе, но при этом, все остальные нелегитимные случаи, которые описаны в модели 1 и модели 2, будут упущены. Но если в организации сложится ситуация, что сотрудник уходит в отпуск или больничный на длительный срок, соответственно его устройство будет неактивно продолжительный период и при первом включении модель определит это устройство как нерегламентированное.

Модель 4. При наличии координат приемника(ов) и интенсивности сигналов на каждой частоте возможно достаточно точно определить координаты источника сигнала. Соответственно зная легитимные устройства модель может работать по следующему правилу: если координаты источника излучения не совпадают с координатами легитимного технического средства, то такое излучение считается нелегитимным.

Данная модель обладает рядом проблем, в первую очередь это точность работы алгоритмов, которые будут вычислять координаты источников сигнала. Другой немаловажной проблемой может быть факт того, что устройства несанкционированного доступа могут встраиваться в легитимные технические средства, соответственно такое излучение модель определит как легитимное.

Для повышения точности обнаружения технических каналов утечки информации предлагается гибридная система, которая объединяет результаты работы моделей 1–4. Каждая модель анализирует определенный аспект сигналов (частотный диапазон, временные

характеристики, периодичность, геолокация), а их результаты агрегируются с использованием метода взвешенного голосования. Это позволяет минимизировать ошибки отдельных моделей и повысить общую надежность системы.

Заключение

В данной работе предложен новый подход к решению задачи поиска технических каналов утечки информации, основанный на использовании методов машинного обучения. Научная новизна исследования заключается в разработке гибридной системы, которая объединяет несколько моделей классификации для анализа различных аспектов радиочастотных сигналов: частотного диапазона, временных характеристик, периодичности и геолокации источников. Данный подход позволяет значительно повысить точность обнаружения и минимизировать количество ложных срабатываний.

Практическая значимость работы заключается в представлении концепции экономически эффективного решения, которое может быть интегрировано в существующие программно-аппаратные комплексы. Перспективы дальнейших исследований включают расширение набора признаков для анализа, создание минимально жизнеспособного продукта, а также разработку междисциплинарного подхода, объединяющего методы машинного обучения, радиофизики и кибербезопасности.

ЛИТЕРАТУРА

1. Belyaev D.O. Hidden technical channels of information leakage: terminology, classification / D.O. Belyaev // 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). — IEEE, 2021. — URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9454994.
2. Рушечников Я.И. Информационная технология радиомониторинга на основе программно-определяемой радиосистемы / Я.И. Рушечников, В.В. Данилов // Вестник ДонНУ. Сер. Г: Технические науки. — 2020. — № 1. — С. 31–36.
3. Короткова А.А. Применение методов машинного обучения в области инженерно-технической защиты информации / А.А. Короткова, С.В. Бобылева // Системный анализ в науке и образовании: сетевое научное издание. — 2023. — № 2. — С. 45–55. — EDN: GYUROT. — URL: https://sanse.ru/index.php/sanse/article/view/578.
4. Сидоркина И.Г. Уточнение классификации технических каналов утечки информации по физической природе носителя с учётом физических эффектов / И.Г. Сидоркина, В.И. Смирнов — DOI: 10.25686/2306-2819.2020.1.37. // Вестник Поволжского государственного технологического университета. Сер.: Радиотехнические и инфокоммуникационные системы. — 2020. — № 1(45). — С. 37–46.
5. Razumov P.V. Development of an adaptive fuzzy algorithm for identifying technical channels of information leakage / P.V. Razumov [et al.] // Proceedings of Sixth International Congress on Information and Communication Technology: ICICT 2021, London. — Singapore: Springer Singapore, 2021. — Т. 3. — С. 297–305.
6. Porsev I.S. Analysis and control of the effectiveness of information protection against leakage through technical channels based on probabilistic assessment / I.S. Porsev, M.A. Melshiyan, A.V. Dushkin // 2022 Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus). — IEEE, 2022. — URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9755623.

7. Чабанов И.Д. Концептуальная модель программно-аппаратного комплекса по поиску технических каналов утечки информации / И.Д. Чабанов, И.Л. Артемьева, И.В. Костенецкий // Информационная безопасность цифровой экономики: материалы XIX научно-практической конференции. — Новосибирск: СибГУТИ, 2023. — С. 271–275. — EDN: QIMUBC.

8. Чабанов И.Д. Сравнение опасности перехвата обрабатываемой информации при использовании видеоинтерфейсов VGA, DVI и HDMI / И.Д. Чабанов, Д.А. Полянский // Теоретические и прикладные вопросы реализации проектов в области информационной безопасности. — Новосибирск: СибГУТИ, 2021. — С. 13–16. — EDN: XHAJJO.

9. Колесников А.Г. Варианты перехвата сигнала и возможность их реализации в оптоволоконном кабеле / А.Г. Колесников // Наука и образование: актуальные вопросы, достижения и инновации: сборник статей III Международной научно-практической конференции. — Пенза: Наука и Просвещение, 2022. — Ч. 1. — С. 122–124. — EDN: AWUFHH.

10. Bhuyan M.H. Network Anomaly Detection: Methods, Systems and Tools / M.H. Bhuyan [et al.] // IEEE Communications Surveys & Tutorials. — 2021. — Т. 23, № 4. — С. 3037–3076.

Chabanov Ilya Dmitrievich
Far Eastern Federal University, Vladivostok, Russia
E-mail: Chabanov.id@dvfu.ru; slepoivareskyn@gmail.com
RSCI: https://elibrary.ru/author_profile.asp?id=1291373

Analysis and development of models for detection of technical information leakage channels using machine learning

Abstract. The article addresses the challenge of detecting technical channels of information leakage amid increasing sophistication of modern information security threats. The research relevance stems from the need to automate the detection of covert surveillance devices, particularly critical for small and medium enterprises that cannot afford expensive equipment or highly qualified specialists.

The authors analyze existing leakage detection methods, including radio frequency monitoring, electromagnetic field analysis, and power line inspection, identifying their key limitations: expert dependency, high costs, and insufficient adaptability to hidden threats. As a solution, the paper proposes machine learning techniques capable of analyzing anomalies in RF signals without human intervention.

The study examines four classification models in detail, each focusing on different signal parameters: frequency compliance with authorized devices; temporal activity patterns; signal periodicity; emission source localization.

The scientific novelty lies in developing a hybrid system that integrates these models using weighted voting, significantly reducing false positives while improving detection accuracy. The practical significance involves creating a cost-effective solution compatible with existing information protection systems.

Prospects for further research include expanding the set of analyzed features, testing in real conditions and implementation in real practices of organizing information security in enterprises.

Keywords: technical channels of information leakage; machine learning; radio frequency analysis; information protection; monitoring automation; hybrid model; signal anomalies