УДК 004.056 **DOI: 10.34670/AR.2026.99.12.063**

Моделирование угроз информационной безопасности при передаче данных по открытым каналам связи с учетом современных методов перехвата и анализа трафика

Тихомирова Валерия Валериевна

Аспирант,
Нижегородский государственный университет им. Н.И. Лобачевского,
603022, Российская Федерация, Нижний Новгород, просп. Гагарина, 23;
e-mail: zenda67895@gmail.com

Корецкий Александр Васильевич

Аспирант
Кубанский государственный технический университет,
350072, Российская Федерация, Краснодар, ул. Московская, 2;
e-mail: koretskyalexandre@yandex.ru

Петренко Иван Сергеевич

Аспирант
Кубанский государственный технический университет,
350072, Российская Федерация, Краснодар, ул. Московская, 2;
e-mail: 79620257777@mail.ru

Шагин Александр Андреевич

Аспирант
Кубанский государственный технический университет,
350072, Российская Федерация, Краснодар, ул. Московская, 2;
e-mail: S15shagin@gmail.com

Устян Кристина Романовна

Аспирант
Санкт-Петербургский государственный университет
промышленных технологий и дизайна,
191186, Российская Федерация, Санкт-Петербург, ул. Большая Морская, 18;
e-mail: kristina_ustyan@list.ru

Аннотация

Передача данных по открытым каналам связи сопровождается ростом результативности пассивного и активного воздействия со стороны нарушителя, тогда как применяемые модели угроз нередко сохраняют ориентацию на сценарии перехвата

полезной нагрузки и недооценивают методы, работающие с метаданными и статистическими характеристиками шифрованного потока. Расхождение между защищённостью содержимого и наблюдаемостью самого факта и структуры обмена остаётся слабо формализованным. Цель работы – построение авторской расчётной модели, увязывающей вероятность реализации угрозы, условную уязвимость канала и тяжесть ущерба в единый интегральный индикатор риска, чувствительный к угрозам анализа трафика. Применены математическое моделирование риска по мультипликативной схеме, агрегирование по вероятности наступления хотя бы одной угрозы и сценарное моделирование профилей защиты. Расчёт на модельной конфигурации из семи угроз показал, что интегральный риск открытого канала достигает 0,702, причём наибольший вклад вносят пассивный перехват (0,317) и подмена узла маршрута (0,257). Введение типового профиля защиты понижает интегральный риск до 0,215, то есть на 69,4%, однако остаточный риск примерно наполовину формируется угрозами инспекции метаданных и корреляционного анализа потоков, которые шифрование полезной нагрузки не нейтрализует. Усиление профиля доводит снижение до 77,3%, при этом доля трафик-аналитических угроз в остатке не убывает. Сопротивляемость анализа трафика криптографической защите означает, что распознавание соответствующего класса угроз достигается перенастройкой наблюдаемых характеристик потока, а не наращиванием стойкости шифрования.

Для цитирования в научных исследованиях

Тихомирова В.В., Корецкий А.В., Петренко И.С., Шагин А.А., Устян К.Р. Моделирование угроз информационной безопасности при передаче данных по открытым каналам связи с учетом современных методов перехвата и анализа трафика // Экономика: вчера, сегодня, завтра. 2026. Том 16. № 6А. С. 614-623. DOI: 10.34670/AR.2026.99.12.063

Ключевые слова

Информационная безопасность, моделирование угроз, открытые каналы связи, перехват трафика, анализ трафика, интегральный риск, профиль защиты, конфиденциальность передачи данных, криптографическая защита, безопасность сетей.

Введение

Открытые каналы связи остаются основной транспортной средой для значительной части межсетевого обмена, и именно их доступность для наблюдения извне предопределяет повышенную поверхность атаки. Нарушителю, получившему доступ к промежуточному сегменту маршрута, доступен не только захват незащищённой полезной нагрузки, но и реконструкция параметров обмена по косвенным признакам. В. А. Радченко и Э. В. Бирих [Радченко, Бирих, 2025], систематизируя угрозы открытых каналов, относят к наиболее результативным сценарии, не требующие компрометации криптографических примитивов; воздействие смещается с содержимого на сопровождающие его характеристики.

Сложившаяся практика противодействия опирается преимущественно на транспортное шифрование; В. Ф. Антонов [Антонов, 2024] показывает, что криптографическая защита данных, передаваемых по открытым каналам, закрывает задачу конфиденциальности содержимого, оставляя открытым вопрос наблюдаемости трафика как такового. Эмпирические

данные о результативности удалённого перехвата, полученные М. М. Ковцуром с соавторами [Ковцур и др., 2021 подтверждают, что доступ к транзитному трафику достижим без нарушения периметра. Здесь обнаруживается расхождение: защита полезной нагрузки и защита факта, объёма и временно́й структуры обмена решаются разными средствами, а в типовых моделях угроз нередко смешиваются.

Анализ угроз перехвата и сопутствующих методов защиты, выполненный в работе А. Исрафилова, И. С. Дроздова и Д. А. Письменского [Исрафилов и др., 2024], фиксирует смещение инструментария нарушителя в сторону автоматизированной обработки перехваченного потока. Рекомендации по защите от перехвата, сформулированные Р. Д. Сулейменовой с соавторами [Сулейменова и др., 2023], ориентированы преимущественно на канальный и сетевой уровни и в меньшей степени затрагивают противодействие статистическому анализу. Тем самым угрозы, работающие с метаданными шифрованного потока, оказываются представленными в моделях фрагментарно, а их вклад в совокупный риск – недооценённым.

Цель работы – формализовать совокупный риск открытого канала через авторскую расчётную модель, в которой угрозы перехвата и угрозы анализа трафика оцениваются в единой метрике, а эффект защитных мер измеряется по остаточному риску. Постановка задачи требует разведения двух слоёв защищённости – содержимого и наблюдаемости обмена – и количественной оценки того, какая часть риска сохраняется после применения шифрования и смежных мер.

Материалы и методы исследования

Методической рамкой расчёта послужили Методика оценки угроз безопасности информации, утверждённая ФСТЭК России 5 февраля 2021 г., и сведения банка данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru) о тактиках и техниках реализации угроз. Перечень последствий и их тяжесть соотнесены с трёхкомпонентной моделью нарушения конфиденциальности, целостности и доступности, операционализированной А. М. Гельфандом [Гельфанд, 2023] применительно к передаче сообщения. Классификация уязвимостей канала опиралась на ГОСТ Р 56546-2015.

Построена авторская модель риска, в которой каждой угрозе i сопоставлены вероятность попытки реализации p_a, условная вероятность успеха при попытке p_v и нормированная тяжесть ущерба u; базовый индекс риска вычисляется мультипликативно, $R_i = p_a \cdot p_v \cdot u$. Идентификация угроз и их параметризация согласованы с методами, систематизированными К. А. Турянской [Турянская, 2024], а способ оценки актуальности – с методикой, апробированной А. О. Мироновой с соавторами [Миронова и др., 2021]. Интегральный риск канала рассчитан по вероятности наступления хотя бы одной угрозы, $R_\Sigma = 1 - \prod(1 - R_i)$, что исключает простое суммирование и учитывает совместное действие разнородных угроз.

Эффект защиты моделировался понижающим коэффициентом результативности меры k_i, уменьшающим условную уязвимость: $p_v' = p_v \cdot (1 - k_i)$; остаточный индекс $R_i' = R_i \cdot (1 - k_i)$. Числовые ориентиры для k_i соотнесены с математическими методами обеспечения безопасности передачи, рассмотренными Д. Г. Тараном с соавторами [Таран и др., 2025], и с методикой повышения защищённости сети при многоэтапном воздействии, предложенной В. А. Липатниковым с соавторами [Липатников и др., 2024]. Сценарное моделирование охватило три профиля защиты возрастающей полноты; значения параметров заданы как модельные и привязаны к расчётной конфигурации, а не к конкретной системе.

Результаты и обсуждение

Модельная конфигурация включила семь угроз, упорядоченных от воздействия на содержимое к воздействию на наблюдаемые характеристики потока: пассивный перехват незащищённого трафика; активную подмену узла маршрута; понижение версии криптографического протокола; инспекцию пакетов и метаданных средствами глубокого разбора; корреляционный и сигнатурный анализ потоков, сохраняющий результативность при шифровании; эксплуатацию скрытого канала по времени; перехват по побочному электромагнитному излучению. Разграничение содержательного перехвата и анализа трафика опирается на систематизацию методов, выполненную З. М. Шпаковской с соавторами [7 Шпаковская и др., 2023]. Обработка перехваченного потока выступает самостоятельным источником сведений о защищаемом обмене и не требует доступа к содержимому.

Методы анализа трафика, описанные Д. С. Яблоковым [Яблоков, 2024], применимы симметрично – и стороной защиты для обнаружения аномалий, и нарушителем для извлечения сведений из перехваченного. С. Э. Тураев и Д. А. Заколдаев [Тураев, Заколдаев, 2024] относят анализ сетевого трафика к базовому инструментарию кибербезопасности, а Ф. И. Сойфер [Сойфер, 2025] трактует его как проактивный метод обнаружения атак. Возможность извлечения сведений по побочным электромагнитным каналам в современных технологиях передачи, показанная И. В. Трубиным с соавторами [Трубин и др., 2025], учтена при оценке тяжести угрозы физического уровня. Доступность той же инструментальной базы нарушителю повышает условную уязвимость угроз корреляционного анализа и скрытых каналов, что отражено в параметрах модели.

Значения параметров модельной конфигурации и рассчитанный базовый индекс риска по каждой угрозе сведены в единую параметризацию (табл. 1).

Таблица 1 - Параметры угроз и базовый индекс риска модельной конфигурации

Угроза	p_a	p_v	u	R_i
Пассивный перехват незащищённого трафика	0,74	0,68	0,63	0,317
Активная подмена узла маршрута	0,53	0,57	0,85	0,257
Понижение версии криптопротокола	0,38	0,44	0,79	0,132
Инспекция пакетов и метаданных (DPI)	0,66	0,61	0,48	0,193
Корреляционный и сигнатурный анализ потоков	0,49	0,39	0,57	0,109
Скрытый канал по времени	0,27	0,31	0,41	0,034
Перехват по электромагнитному излучению	0,18	0,23	0,66	0,027

Источник: составлено авторами.

Наибольший базовый риск сосредоточен на пассивном перехвате (0,317) и подмене узла (0,257) – угрозах, для которых высоки и вероятность попытки, и условная уязвимость незащищённого канала. Угрозы инспекции метаданных (0,193) и корреляционного анализа потоков (0,109) занимают срединное положение по базовому индексу, однако их особенность в том, что условная уязвимость слабо снижается шифрованием полезной нагрузки. Скрытый временно́й канал (0,034) и перехват по электромагнитному излучению (0,027) дают наименьший базовый вклад, причём у последнего при низкой вероятности высока тяжесть последствий.

Выбранная параметризация отражает асимметрию доступности угроз для нарушителя промежуточного сегмента. Пассивный перехват и инспекция метаданных не требуют активного вмешательства в обмен и потому получают высокую вероятность попытки; подмена узла и

понижение версии протокола предполагают активные действия с риском обнаружения, что отражено пониженной вероятностью попытки при сохранении высокой условной уязвимости. Угрозы физического уровня вынесены в отдельный диапазон значений, поскольку их реализация ограничена пространственной близостью к среде передачи, а тяжесть последствий при успехе сопоставима с прямым перехватом содержимого. Такое разнесение параметров удерживает модель в границах наблюдаемого распределения угроз открытого канала и предотвращает искусственное выравнивание их вкладов.

Интегральный риск канала, рассчитанный по схеме наступления хотя бы одной угрозы, составил 0,702. Аддитивная сумма частных индексов превысила бы единицу (1,07), что лишено вероятностного смысла; мультипликативное агрегирование удерживает оценку в границах [0; 1] и отражает частичное перекрытие зон действия разнородных угроз.

Результат применения типового профиля защиты – сочетания аутентифицированного шифрования, туннелирования и нормализации трафика – выражен через коэффициент результативности меры и остаточный индекс риска по каждой угрозе (табл. 2).

Таблица 2 - Остаточный индекс риска при типовом профиле защиты

Угроза	k_i	R_i'
Пассивный перехват незащищённого трафика	0,92	0,025
Активная подмена узла маршрута	0,86	0,036
Понижение версии криптопротокола	0,81	0,025
Инспекция пакетов и метаданных (DPI)	0,64	0,070
Корреляционный и сигнатурный анализ потоков	0,47	0,058
Скрытый канал по времени	0,58	0,014
Перехват по электромагнитному излучению	0,69	0,008

Источник: составлено авторами.

Типовой профиль понижает интегральный риск с 0,702 до 0,215, относительное снижение – 69,4%. Распределение остатка неравномерно: на инспекцию метаданных (0,070) и корреляционный анализ потоков (0,058) приходится около 54% остаточного аддитивного риска, тогда как до применения мер эти угрозы давали менее трети суммарного индекса. Перераспределение объясняется тем, что результативность шифрования против перехвата содержимого близка к предельной (коэффициент 0,92 для пассивного перехвата), а против анализа наблюдаемых характеристик ограничена (0,47 для корреляционного анализа), поскольку дополнение и нормализация потока скрывают его структуру лишь частично.

Полученное смещение, по всей видимости, отражает устойчивую закономерность: меры, адресованные конфиденциальности содержимого, и меры, адресованные наблюдаемости обмена, обладают разной предельной результативностью. Вероятно, именно поэтому наращивание стойкости криптографической защиты после некоторого порога перестаёт понижать совокупный риск.

Практическое прочтение перераспределения остатка состоит в смене приоритета защитных вложений. Пока доминируют угрозы перехвата содержимого, прирост стойкости шифрования окупается заметным понижением совокупного риска; после нейтрализации этого слоя дополнительные вложения в криптографию дают убывающую отдачу, а ведущим фактором понижения становится результативность маскирования наблюдаемых характеристик потока. Модель позволяет оценить порог, за которым целесообразен переход от усиления шифрования к мерам выравнивания трафика, по точке, в которой остаточный вклад инспекции метаданных и корреляционного анализа начинает превышать вклад прямого перехвата. В рассмотренной

конфигурации этот порог достигается уже в пределах типового профиля защиты.

Сопоставление трёх профилей защиты возрастающей полноты по интегральному риску и относительному снижению приведено в сравнительной форме (табл. 3).

Таблица 3 - Интегральный риск канала при разных профилях защиты

Профиль защиты	R_Σ	Снижение относительно базового, %
Без мер защиты (базовый)	0,702	–
Только транспортное шифрование (TLS 1.3)	0,338	51,8
Типовой (шифрование, туннелирование, нормализация)	0,215	69,4
Усиленный (типовой, экранирование, дополнение трафика)	0,159	77,3

Источник: составлено авторами.

Переход от незащищённого канала к транспортному шифрованию снимает чуть более половины интегрального риска (до 0,338), однако дальнейшие приращения защищённости убывают: типовой профиль добавляет 17,6 процентного пункта снижения, усиленный – ещё 7,9. Кривая результативности уплощается, и причина уплощения локализуется в трафик-аналитическом классе угроз. Даже усиленный профиль, доводящий снижение до 77,3%, оставляет остаточный риск 0,159, в котором доля инспекции метаданных и корреляционного анализа относительно прочих составляющих растёт.

Расхождение результативности мер против двух слоёв защищённости – содержимого и наблюдаемости – выражается количественно: коэффициент для пассивного перехвата близок к единице во всех профилях, тогда как для корреляционного анализа он не превышает 0,66 даже при усиленной нормализации. Отсюда вытекает, что предельно достижимое снижение совокупного риска ограничено сверху результативностью маскирования наблюдаемых характеристик потока, тогда как стойкость шифрования этот предел не сдвигает.

Сложившаяся в моделях угроз ориентация на защиту содержимого недооценивает остаточный риск, локализованный в анализе трафика. Количественно этот риск не исчезает при наращивании криптографической стойкости и сохраняет долю порядка половины остатка при любом из рассмотренных профилей. Распознавание угроз соответствующего класса достигается перенастройкой наблюдаемых параметров потока: выравниванием размеров и темпа следования пакетов, внесением управляемых задержек. Усиление шифрования на этот слой риска не действует.

Заключение

На модельной конфигурации из семи угроз совокупный риск передачи по открытому каналу, сведённый к единому интегральному индикатору, превысил 0,7. Основная его часть до применения защиты приходится на прямой перехват, тогда как трафик-аналитические угрозы занимают срединные позиции.

После введения защитных мер обнаруживается принципиальное смещение. Типовой профиль понижает интегральный риск примерно на 69%, доводя его до значений около 0,22, однако внутренняя структура остатка меняется качественно: угрозы, работающие с метаданными и статистической структурой шифрованного потока, начинают доминировать и удерживают около половины остаточного риска. Усиление профиля доводит относительное снижение до значений свыше 77%, но соотношение в остатке не меняет – доля анализа трафика не убывает. Полученная картина указывает на разную предельную результативность двух

семейств мер: защита содержимого приближается к насыщению уже при транспортном шифровании, тогда как маскирование наблюдаемых характеристик обмена остаётся частичным даже при дополнении и нормализации потока. Отсюда верхняя граница достижимого снижения совокупного риска задаётся не стойкостью криптографических примитивов, а результативностью сокрытия факта, объёма и временно́й структуры передачи.

Теоретически это разводит две задачи, нередко смешиваемые в моделях угроз открытого канала, – защиту конфиденциальности содержимого и защиту наблюдаемости обмена. Расхождение, обозначенное во введении между стойкостью шифрования и информативностью перехваченного потока, получает количественное выражение: после нейтрализации содержательного перехвата риск концентрируется в слое, к которому шифрование нечувствительно.

Благодаря мультипликативной схеме агрегирования интегральная оценка удерживается в вероятностных границах и не завышается относительно аддитивного суммирования, которое на той же конфигурации превышает единицу. Разнесение вероятности попытки, условной уязвимости и тяжести ущерба позволяет локализовать вклад каждой угрозы и проследить, как профиль защиты перераспределяет совокупный риск, понижая его лишь частично.

Распознавание трафик-аналитических угроз достигается перенастройкой наблюдаемых параметров потока; усиление криптографической стойкости в этом слое риска не помогает, и именно здесь сохраняется остаточный риск порядка 0,16 при наиболее полном из рассмотренных профилей защиты.

Библиография

1. Антонов В.Ф. Разработка системы криптографической защиты информации, передаваемой по открытым каналам связи // Современная наука и инновации. 2024. № 4 (48). С. 22–28.
2. Гельфанд А.М. Модель угроз конфиденциальности, целостности и доступности при передаче сообщения // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2023. № 2. С. 5–9.
3. Исрафилов А., Дроздов И.С., Письменский Д.А. Анализ угроз перехвата трафика и эффективные методы защиты // Дневник науки. 2024. № 4 (88).
4. Ковцур М.М., Герлинг Е.Ю., Коновалова В.В., Кистуга А.Ю. Исследование способов удаленного перехвата трафика в корпоративных сетях // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. № 4. С. 68–75.
5. Липатников В.А., Шевченко А.А., Мелехов К.В., Ткачев Д.Ф. Методика повышения защищенности сети передачи данных объектов критической информационной инфраструктуры при многоэтапных атаках // Информационно-управляющие системы. 2024. № 1 (128). С. 44–55.
6. Миронова А.О., Гончаренко Ю.Ю., Гоголь А.С., Фролова А.Н. Применение методики оценки угроз безопасности информации // Энергетические установки и технологии. 2021. Т. 7. № 4. С. 71–75.
7. Радченко В.А., Бирих Э.В. Методы защиты и предотвращения угроз в открытых каналах связи // Актуальные проблемы социально-гуманитарного и научно-технического знания. 2025. № 1 (41). С. 17–19.
8. Сойфер Ф.И. Анализ сетевого трафика как проактивный метод обнаружения атак // Международный журнал информационных технологий и энергоэффективности. 2025. Т. 10. № 9 (59). С. 5–11.
9. Сулейменова Р.Д., Неплях Т.В., Шинкаренко Д.А. Рекомендации по обеспечению безопасности от возможного перехвата трафика // Наукосфера. 2023. № 4-1. С. 250–255.
10. Таран Д.Г., Мартынов А.С., Шабардин А.С. Математические методы обеспечения информационной безопасности при передаче данных // Труды международного симпозиума «Надежность и качество». 2025. Т. 1. С. 248–251.
11. Трубин И.В., Наборщикова А.Д., Чернышев П.Р. Анализ каналов утечки информации на основе электромагнитных сигналов радиодиапазона в современных технологиях передачи данных // Безопасность цифровых технологий. 2025. № 1 (116). С. 53–69.
12. Тураев С.Э., Заколдаев Д.А. Анализ сетевого трафика (АСТ) в кибербезопасности // Наука и бизнес: пути развития. 2024. № 5 (155). С. 61–65.
13. Турянская К.А. Методы, модели и средства выявления, идентификации и классификации угроз нарушения

информационной безопасности объектов различного вида и класса // Международный журнал гуманитарных и естественных наук. 2024. № 2-2 (89). С. 151–155.
14. Шпаковская З.М., Фалалеева М.А., Сулейменова Р.Д. Сетевой трафик, методы его анализа и применение в информационной безопасности // Наукосфера. 2023. № 4-2. С. 316–320.
15. Яблоков Д.С. Методы анализа сетевого трафика // Тенденции развития науки и образования. 2024. № 114-9. С. 163–166.

Modeling of Information Security Threats in Data Transmission over Open Communication Channels with Regard to Modern Methods of Interception and Traffic Analysis

Valeriya V. Tikhomirova

Postgraduate Student,
N.I. Lobachevsky National Research Nizhny Novgorod State University,
603022, 23, Gagarina ave., Nizhny Novgorod, Russian Federation;
e-mail: zenda67895@gmail.com

Aleksandr V. Koretskii

Postgraduate Student,
Kuban State Technological University,
350072, 2, Moskovskaya str., Krasnodar, Russian Federation;
e-mail: koretskyalexandre@yandex.ru

Ivan S. Petrenko

Postgraduate Student,
Kuban State Technological University,
350072, 2, Moskovskaya str., Krasnodar, Russian Federation;
e-mail: 79620257777@mail.ru

Aleksandr A. Shagin

Postgraduate Student,
Kuban State Technological University,
350072, 2, Moskovskaya str., Krasnodar, Russian Federation;
e-mail: S15shagin@gmail.com

Kristina R. Ustyan

Postgraduate Student,
Saint Petersburg State University of Industrial Technologies and Design,
191186, 18, Bol'shaya Morskaya str., Saint Petersburg, Russian Federation;
e-mail: kristina_ustyan@list.ru

Abstract

Data transmission over open communication channels is accompanied by an increase in the effectiveness of passive and active influence on the part of the intruder, while the applied threat models often remain oriented towards scenarios of payload interception and underestimate methods working with metadata and statistical characteristics of the encrypted flow. The discrepancy between the security of content and the observability of the very fact and structure of the exchange remains poorly formalized. The objective of the work is to build an author's calculation model linking the probability of threat realization, the conditional vulnerability of the channel, and the severity of damage into a single integral risk indicator sensitive to traffic analysis threats. Mathematical modeling of risk according to a multiplicative scheme, aggregation by the probability of occurrence of at least one threat, and scenario modeling of protection profiles were applied. Calculation on a model configuration of seven threats showed that the integral risk of an open channel reaches 0.702, with the largest contribution made by passive interception (0.317) and route node substitution (0.257). The introduction of a standard protection profile reduces the integral risk to 0.215, i.e., by 69.4%; however, the residual risk is approximately half formed by threats of metadata inspection and correlation analysis of flows, which payload encryption does not neutralize. Strengthening the profile brings the reduction to 77.3%, while the share of traffic-analytical threats in the remainder does not decrease. The resistance of traffic analysis to cryptographic protection means that the recognition of the corresponding class of threats is achieved by reconfiguring the observable flow characteristics rather than by increasing encryption strength.

For citation

Tikhomirova V.V., Koretskii A.V., Petrenko I.S., Shagin A.A., Ustyan K.R. (2026) Modelirovanie ugroz informatsionnoy bezopasnosti pri peredache dannykh po otkrytym kanalam svyazi s uchetom sovremennykh metodov perekhvata i analiza trafika [Modeling of Information Security Threats in Data Transmission over Open Communication Channels with Regard to Modern Methods of Interception and Traffic Analysis]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 16 (6A), pp. 614-623. DOI: 10.34670/AR.2026.99.12.063

Keywords

Information security, threat modeling, open communication channels, traffic interception, traffic analysis, integral risk, protection profile, data transmission confidentiality, cryptographic protection, network security.

References

1. Antonov, V. F. (2024). Razrabotka sistemy kriptograficheskoy zashchity informatsii, peredavayemoy po otkrytym kanalam svyazi [Development of a cryptographic protection system for information transmitted over open communication channels]. Sovremennaya nauka i innovatsii [Modern Science and Innovations], *4*(48), 22–28.
2. Gelfand, A. M. (2023). Model' ugroz konfidentsial'nosti, tselostnosti i dostupnosti pri peredache soobshcheniya [A model of threats to confidentiality, integrity and availability in message transmission]. Vestnik Sankt-Peterburgskogo gosudarstvennogo universiteta tekhnologii i dizayna. Seriya 1: Yestestvennyye i tekhnicheskiye nauki [Bulletin of St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences], *2*, 5–9.
3. Israfilov, A., Drozdov, I. S., & Pismenskiy, D. A. (2024). Analiz ugroz perekhvata trafika i effektivnyye metody zashchity [Analysis of traffic interception threats and effective protection methods]. Dnevnik nauki [Diary of Science], *4*(88).
4. Kovtsur, M. M., Gerling, E. Yu., Konovalova, V. V., & Kistruga, A. Yu. (2021). Issledovaniye sposobov udalennogo perekhvata trafika v korporativnykh setyakh [A study of methods of remote traffic interception in corporate networks]. Vestnik Sankt-Peterburgskogo gosudarstvennogo universiteta tekhnologii i dizayna. Seriya 1: Yestestvennyye i tekhnicheskiye nauki [Bulletin of St. Petersburg State University of Technology and Design. Series 1:

Natural and Technical Sciences], *4*, 68–75.
5. Lipatnikov, V. A., Shevchenko, A. A., Melekhov, K. V., & Tkachev, D. F. (2024). Metodika povysheniya zashchishchennosti seti peredachi dannykh ob"yektov kriticheskoy informatsionnoy infrastruktury pri mnogoetapnykh atakakh [A methodology for increasing the security of a data transmission network of critical information infrastructure objects under multi-stage attacks]. Informatsionno-upravlyayushchiye sistemy [Information and Control Systems], *1*(128), 44–55.
6. Mironova, A. O., Goncharenko, Yu. Yu., Gogol, A. S., & Frolova, A. N. (2021). Primeneniye metodiki otsenki ugroz bezopasnosti informatsii [Application of a methodology for assessing information security threats]. Energeticheskiye ustanovki i tekhnologii [Power Plants and Technologies], *7*(4), 71–75.
7. Radchenko, V. A., & Birikh, E. V. (2025). Metody zashchity i predotvrashcheniya ugroz v otkrytykh kanalakh svyazi [Methods of protection and prevention of threats in open communication channels]. Aktual'nyye problemy sotsial'no-gumanitarnogo i nauchno-tekhnicheskogo znaniya [Topical Issues of Socio-Humanitarian and Scientific-Technical Knowledge], *1*(41), 17–19.
8. Soyfer, F. I. (2025). Analiz setevogo trafika kak proaktivnyy metod obnaruzheniya atak [Network traffic analysis as a proactive method of attack detection]. Mezhdunarodnyy zhurnal informatsionnykh tekhnologiy i energoeffektivnosti [International Journal of Information Technologies and Energy Efficiency], *10*(9), 5–11.
9. Suleymenova, R. D., Neplyakh, T. V., & Shinkarenko, D. A. (2023). Rekomendatsii po obespecheniyu bezopasnosti ot vozmozhnogo perekhvata trafika [Recommendations for ensuring security against possible traffic interception]. Naukosfera [Naukosphere], *4-1*, 250–255.
10. Taran, D. G., Martynov, A. S., & Shabardin, A. S. (2025). Matematicheskiye metody obespecheniya informatsionnoy bezopasnosti pri peredache dannykh [Mathematical methods of ensuring information security in data transmission]. In Trudy mezhdunarodnogo simpoziuma "Nadezhnost' i kachestvo" [Proceedings of the International Symposium "Reliability and Quality"] (Vol. 1, pp. 248–251).
11. Trubin, I. V., Naborshchikova, A. D., & Chernyshev, P. R. (2025). Analiz kanalov utechki informatsii na osnove elektromagnitnykh signalov radiodiapazona v sovremennykh tekhnologiyakh peredachi dannykh [Analysis of information leakage channels based on radio-range electromagnetic signals in modern data transmission technologies]. Bezopasnost' tsifrovykh tekhnologiy [Security of Digital Technologies], *1*(116), 53–69.
12. Turaev, S. E., & Zakoldaev, D. A. (2024). Analiz setevogo trafika (AST) v kiberbezopasnosti [Network traffic analysis in cybersecurity]. Nauka i biznes: puti razvitiya [Science and Business: Ways of Development], *5*(155), 61–65.
13. Turyanskaya, K. A. (2024). Metody, modeli i sredstva vyyavleniya, identifikatsii i klassifikatsii ugroz narusheniya informatsionnoy bezopasnosti ob"yektov razlichnogo vida i klassa [Methods, models and means of detecting, identifying and classifying information security violation threats to objects of various types and classes]. Mezhdunarodnyy zhurnal gumanitarnykh i yestestvennykh nauk [International Journal of Humanities and Natural Sciences], *2-2*(89), 151–155.
14. Shpakovskaya, Z. M., Falaleeva, M. A., & Suleymenova, R. D. (2023). Setevoy trafik, metody yego analiza i primeneniye v informatsionnoy bezopasnosti [Network traffic, methods of its analysis and application in information security]. Naukosfera [Naukosphere], *4-2*, 316–320.
15. Yablokov, D. S. (2024). Metody analiza setevogo trafika [Methods of network traffic analysis]. Tendentsii razvitiya nauki i obrazovaniya [Trends in the Development of Science and Education], *114-9*, 163–166.