УДК 004.056:621.396.2

Лебедев Иван Владимирович

Аспирант первого курса, кафедры отечественные сети магистральной связи, факультет сети и системы связи

Московский технический университет связи и информатики, 111024, РФ, г. Москва, ул. Авиамоторная, д. 8А

МЕТОДЫ ОБЕСПЕЧЕНИЯ КИБЕРУСТОЙЧИВОСТИ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ УПРАВЛЕНИЯ КАНАЛАМИ СВЯЗИ ПРИ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ

Аннотация

Статья посвящена исследованию методов обеспечения киберустойчивости интеллектуальных систем управления каналами связи, применяемых в комплексах экстренного оповещения населения при чрезвычайных ситуациях. Актуальность работы определяется тем, что цифровизация и интеллектуализация систем оповещения, расширяя их функциональные возможности, одновременно формируют новую поверхность атаки, эксплуатация которой в условиях кризиса способна привести к полному прекращению оповещения или дезинформации населения. Проблема исследования состоит в отсутствии систематизированного подхода к обеспечению кибербезопасности именно интеллектуального компонента — модуля прогнозирования и принятия решений о выборе канала. В работе проведён анализ актуальной модели угроз для таких систем, включающей атаки на каналы телеметрии, атаки типа «отравление данных» на прогнозные модели, атаки на управляющую инфраструктуру и угрозы социальной инженерии. На основании анализа предложен комплекс технических и

организационных методов противодействия, включающий криптографическую защиту служебного трафика, механизмы обнаружения аномалий во входящей телеметрии, архитектурный принцип безопасного отказа и многоуровневую сегментацию сети. Рассматриваются перспективы применения методов федеративного обучения для повышения устойчивости прогнозных моделей к состязательным воздействиям.

Ключевые слова: киберустойчивость, системы экстренного оповещения, интеллектуальное управление каналами связи, атака «отравление данных», обнаружение аномалий, безопасный отказ, КСЭОН, кибербезопасность критической инфраструктуры, ФСТЭК.

Annotation

The article examines methods for ensuring the cyber resilience of intelligent communication channel management systems used in emergency public notification complexes during emergency situations. The relevance of the work is determined by the fact that the digitalization and intellectualization of notification systems, while expanding their functional capabilities, simultaneously form a new attack surface, the exploitation of which during a crisis can lead to a complete cessation of notification or misinformation of the population. The research problem lies in the absence of a systematized approach to ensuring cybersecurity specifically of the intelligent component — the forecasting and channel selection decision-making module. The paper analyzes the current threat model for such systems, including attacks on telemetry channels, data poisoning attacks on predictive models, attacks on control infrastructure, and social engineering threats. Based on the analysis, a set of technical and organizational countermeasures is proposed, including cryptographic protection of service traffic, anomaly detection mechanisms for incoming telemetry, the architectural principle of safe failure, and multi-level

network segmentation. The prospects for using federated learning methods to increase the resilience of predictive models to adversarial influences are considered.

Keywords: cyber resilience, emergency notification systems, intelligent communication channel management, data poisoning attack, anomaly detection, safe failure, CCEP, critical infrastructure cybersecurity, FSTEC.

Цель исследования – систематизировать и обосновать методы обеспечения киберустойчивости интеллектуальных систем управления каналами связи, применяемых в комплексах экстренного оповещения населения при чрезвычайных ситуациях.

Проблема исследования состоит в том, что переход систем оповещения к интеллектуальной, управляемой данными парадигме порождает качественно новую категорию уязвимостей, не характерных для традиционных детерминированных схем резервирования. Если в статической системе отказ одного компонента влечёт предсказуемые и заранее учтённые последствия, то в адаптивной системе целенаправленное воздействие на алгоритм принятия решений способно незаметно привести к выбору заведомо деградированного канала в самый критический момент. Такая атака может вообще не проявляться в штатном режиме и стать очевидной лишь в условиях реальной чрезвычайной ситуации, когда возможности для корректирующих мер минимальны [1, 2].

Между тем нормативная база в сфере кибербезопасности критической информационной инфраструктуры — Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры» и приказы ФСТЭК России — формирует общие требования к защите значимых объектов, не специфицируя меры

применительно к интеллектуальным компонентам систем оповещения [3, 4]. Это создаёт методологический пробел, который настоящее исследование призвано частично восполнить.

Модель угроз для интеллектуальных систем управления каналами связи.

Построение адекватной системы защиты невозможно без предварительной формализации модели угроз. Применительно к интеллектуальным системам управления каналами связи целесообразно выделить четыре основных класса угроз, различающихся по точке приложения воздействия и потенциальным последствиям.

Атаки на каналы телеметрии направлены на компрометацию потоков данных, поступающих от модуля мониторинга в модуль прогнозирования. Нарушитель, получивший возможность модифицировать или подменять показатели качества обслуживания — задержку, коэффициент потерь пакетов, доступность — способен сформировать у системы ложное представление о состоянии сети. Следствием становится систематически неверный выбор основного канала: система будет направлять критически важный трафик оповещения через деградированный или контролируемый нарушителем путь [5, 6].

Атаки типа «отравление данных» (data poisoning) представляют собой специфическую угрозу для машинно-обучаемых прогнозных компонентов. В отличие от атак на телеметрию, действующих в реальном времени, данный класс атак реализуется на этапе обучения модели путём внесения целенаправленных искажений в обучающую выборку. Результатом является модель, демонстрирующая корректное поведение при штатных условиях, но систематически ошибающаяся в специфических сценариях, соответствующих условиям ЧС. Выявление

подобных атак существенно затруднено ввиду отсроченного проявления их последствий [5, 7].

Атаки на управляющую инфраструктуру нацелены на непосредственное воздействие на компоненты, реализующие решения о коммутации трафика: SDN-контроллеры, сетевые шлюзы, серверы рассылки. Несанкционированный доступ к этим элементам позволяет нарушителю либо заблокировать исполнение легитимных команд, либо инициировать ложный запуск оповещения с дезинформирующим содержимым. Оба сценария несут непосредственную угрозу жизни и здоровью людей [4, 6].

Угрозы социальной инженерии применительно к рассматриваемым системам сводятся прежде всего к компрометации учётных данных персонала дежурно-диспетчерских служб, имеющего санкционированный доступ к управляющим компонентам. Данный вектор атаки зачастую недооценивается при проектировании технических мер защиты, однако именно он исторически обеспечивал наиболее результативные проникновения в критическую инфраструктуру [3, 8].

Криптографическая защита служебного трафика и сегментация сети.

Базовым методом противодействия атакам на каналы телеметрии является обеспечение конфиденциальности и целостности потоков мониторинговых данных. Для этого весь служебный трафик между агентами мониторинга и центральным модулем прогнозирования должен передаваться по защищённым каналам с применением криптографических алгоритмов, соответствующих требованиям ГОСТ Р 34.12-2015 [3, 9]. Взаимная аутентификация узлов на основе сертификатов X.509 исключает подключение несанкционированных

агентов мониторинга или подмену центрального сервера прогнозирования.

Принципиально важным архитектурным решением является физическая и логическая изоляция служебного трафика от пользовательского сегмента сети. Реализуется она посредством VLAN-сегментации: управляющий трафик модуля принятия решений, телеметрия мониторинга и трафик оповещения разносятся по отдельным виртуальным сетям с разграничительными политиками межсетевого экранирования. Межсетевые экраны уровня приложений (NGFW) обеспечивают инспекцию трафика управляющих протоколов и блокируют нетипичные обращения к управляющим интерфейсам SDN-контроллеров. Системы обнаружения и предотвращения вторжений (IDS/IPS), интегрированные в управляющий сегмент, ведут непрерывный анализ сетевой активности на предмет аномальных паттернов [6, 8].

Разграничение доступа к управляющим компонентам строится на принципе наименьших привилегий с применением ролевой модели (RBAC). Каждая служебная учётная запись наделяется исключительно теми правами, которые необходимы для выполнения соответствующей функции, что существенно ограничивает возможный ущерб в случае компрометации одной из учётных записей. Привилегированный доступ к управляющей инфраструктуре должен осуществляться исключительно через защищённые шлюзы с многофакторной аутентификацией и обязательным журналированием всех действий [4, 9].

Обнаружение аномалий во входящей телеметрии.

Поскольку криптографическая защита канала телеметрии не исключает компрометации самих агентов мониторинга, необходим второй рубеж защиты — контроль статистической достоверности поступающих данных. Центральная идея состоит в том, что легитимные

показатели качества канала связи подчиняются определённым статистическим закономерностям, обусловленным физическими характеристиками среды передачи и типичными паттернами сетевой нагрузки. Аномально резкие изменения метрик, не коррелирующие с наблюдаемыми изменениями в смежных каналах или внешними событиями, с высокой вероятностью свидетельствуют о компрометации источника данных, а не об объективном изменении состояния сети [5, 7].

Для формализации этого подхода рассмотрим вектор состояния канала в момент времени t:

$$S_i(t) = (A_i(t), L_i(t), P_i(t), J_i(t)),$$

где $A_i(t)$ — доступность, $L_i(t)$ — задержка, $P_i(t)$ — потери пакетов, $J_i(t)$ — джиттер. Показатель аномальности компоненты k вектора состояния может быть оценён через стандартизованное отклонение от скользящего среднего:

$$\Delta_{ik}(t) = |s_{ik}(t) - \mu_{ik}| / \sigma_{ik},$$

где μ_{ik} и σ_{ik} — скользящее среднее и среднеквадратическое отклонение компоненты k для канала i, вычисленные на скользящем окне наблюдений. При превышении показателем $\Delta_{ik}(t)$ порогового значения δ_a соответствующее наблюдение помечается как потенциально скомпрометированное и исключается из расчёта интегрального показателя качества. Дополнительно анализируется межканальная корреляция: резкое ухудшение параметров одного канала при неизменном состоянии физически независимых каналов указывает на локальный источник аномалии — будь то реальный отказ конкретного оборудования или атака на агент мониторинга [5, 10].

Для выявления атак типа «отравление данных» на прогнозные модели применяется периодическая верификация модели на контрольной выборке с эталонными характеристиками, сформированной в доверенной среде и хранящейся в зашифрованном

виде. Существенное отклонение метрик точности модели от эталонных значений служит сигналом о возможной компрометации обучающих данных и инициирует откат к предыдущей верифицированной версии модели [7, 11].

Принцип безопасного отказа и детерминированный резервный режим.

Ни один из описанных методов обнаружения угроз не обеспечивает абсолютной надёжности — всегда существует ненулевая вероятность как ложноположительного, так и ложноотрицательного срабатывания. В условиях критической инфраструктуры это предопределяет необходимость реализации принципа безопасного отказа (fail-safe), согласно которому при любом неопределённом или подозрительном состоянии системы она должна переходить в наиболее безопасный из доступных режимов работы, а не продолжать функционирование с возможно скомпрометированными данными [4, 6].

Применительно к интеллектуальной системе управления каналами связи это означает наличие полностью детерминированного резервного режима, не зависящего от прогнозных моделей и входящей телеметрии. В данном режиме выбор канала осуществляется по жёстко заданной статической таблице приоритетов, основанной на априорных, верифицированных данных о надёжности каждого канала в конкретной инфраструктурной среде. Такой режим заведомо уступает интеллектуальному по эффективности при штатных условиях, однако обеспечивает предсказуемое и защищённое поведение системы при подтверждённом или подозреваемом кибервоздействии [2, 8].

Переход в детерминированный резервный режим инициируется при выполнении одного из следующих условий: устойчивое превышение порога аномальности $\Delta_{ik}(t) > \delta_a$ для критической доли каналов телеметрии; обнаружение нетипичных команд управления в

журналах IDS/IPS; отклонение метрик точности прогнозных моделей от эталонных значений сверх допустимого предела; обнаружение попытки несанкционированного доступа к компонентам управляющей инфраструктуры. Выход из резервного режима возможен только после завершения процедуры верификации целостности всех компонентов системы уполномоченным персоналом, что исключает автоматический возврат к работе с потенциально скомпрометированными данными [3, 9].

Организационные меры и непрерывный аудит безопасности.

Технические меры кибербезопасности не могут рассматриваться в отрыве от организационных. Как показывает практика реагирования на инциденты с объектами критической инфраструктуры, значительная их часть стала возможной не вследствие технических уязвимостей, а в результате нарушения регламентов эксплуатации или компрометации персонала [3, 8]. Применительно к системам оповещения данный риск усиливается тем, что дежурный персонал ЕДДС в условиях ЧС действует в состоянии стресса и при дефиците времени, что снижает бдительность в отношении нетипичных запросов.

К обязательным организационным мерам относятся: регулярное обучение персонала методам распознавания атак социальной инженерии с проведением контрольных учений; ведение и анализ журналов всех действий с привилегированными учётными записями; регламентированный порядок реагирования на инциденты кибербезопасности с чётко определёнными зонами ответственности; периодическое проведение тестирования на проникновение с обязательным охватом интеллектуальных компонентов системы. Разработка и поддержание в актуальном состоянии модели угроз, учитывающей не только технические, но и сценарные аспекты (типы

нарушителей, их мотивацию и возможности), является необходимым условием адекватности всего комплекса мер защиты [4, 10].

Непрерывный аудит безопасности предполагает автоматизированный сбор и корреляцию событий безопасности из всех компонентов системы в рамках единой платформы управления информацией и событиями безопасности (SIEM). Корреляционные правила платформы настраиваются с учётом специфики рассматриваемых угроз: например, одновременное ухудшение телеметрии нескольких каналов разных операторов в сочетании с попытками нетипичного доступа к управляющим интерфейсам должно автоматически генерировать высокоприоритетный инцидент и инициировать переход в детерминированный резервный режим [6, 11].

Перспективные методы повышения устойчивости прогнозных моделей.

Описанные методы противодействия атакам на прогнозные компоненты основаны на внешнем контроле целостности данных и не затрагивают фундаментальной уязвимости централизованного обучения: всё множество обучающих данных аккумулируется в одном месте, что само по себе является точкой концентрации риска. Методология федеративного обучения (Federated Learning) предлагает принципиально иной подход: модели обучаются локально на каждом из агентов мониторинга, а в центральный сервер передаются только параметры обновления — градиенты или веса модели, но никак не сырые данные. Это существенно усложняет проведение атак типа «отравление данных», поскольку компрометация одного агента оказывает лишь ограниченное влияние на глобальную модель [7, 11].

Методы состязательного обучения (Adversarial Training) предполагают включение в обучающую выборку синтетических атакующих примеров, что повышает устойчивость модели к ранее не

наблюдавшимся паттернам воздействия. Регуляризирующие техники, в частности дифференциальная приватность при обновлении параметров, ограничивают влияние отдельных наблюдений на итоговую модель, снижая тем самым эффективность целенаправленных манипуляций с обучающей выборкой. Совокупное применение этих методов формирует многорубежную защиту интеллектуальных компонентов — от уровня данных до уровня архитектуры модели [5, 7].

Вместе с тем необходимо учитывать, что все перечисленные методы сопряжены с определёнными накладными расходами — вычислительными, коммуникационными или в части точности прогнозирования. Оптимальный баланс между достигаемым уровнем киберустойчивости и эксплуатационными издержками должен определяться для каждой конкретной инфраструктурной среды на основе количественного анализа рисков с учётом нормативных требований к системам оповещения [3, 10].

Таким образом, в ходе проведённого исследования систематизированы методы обеспечения киберустойчивости интеллектуальных систем управления каналами связи при чрезвычайных ситуациях. Показано, что интеллектуализация систем оповещения сопряжена с возникновением специфических угроз — прежде всего атак на каналы телеметрии и атак типа «отравление данных» на прогнозные компоненты, — противодействие которым требует специальных методов, выходящих за рамки стандартных мер защиты периметра сети. Предложенный комплекс мер охватывает четыре уровня: криптографическую защиту и сегментацию служебного трафика; статистический контроль достоверности входящей телеметрии; архитектурный принцип безопасного отказа с детерминированным резервным режимом; организационные меры и непрерывный аудит безопасности. Дополнительным перспективным направлением является

применение методов федеративного и состязательного обучения для повышения априорной устойчивости прогнозных моделей к состязательным воздействиям. Совокупная реализация описанных методов позволяет сформировать многорубежную систему защиты, сохраняющую работоспособность системы оповещения даже в условиях активного противодействия нарушителя.

Литература

1. О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон от 26.07.2017 № 187-ФЗ // Собрание законодательства РФ. – 2017. – № 31 (ч. I). – Ст. 4736.

2. Об утверждении Положения о системах оповещения населения : постановление Правительства РФ от 01.03.2019 № 1074 (ред. от 23.10.2021) // Собрание законодательства РФ. – 2019. – № 10. – Ст. 1028.

3. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации : приказ ФСТЭК России от 25.12.2017 № 239. – М., 2017.

4. Ахмедова Х. М. Организационно-правовое регулирование информирования и оповещения населения при угрозе и возникновении чрезвычайных ситуаций природного или техногенного характера // Молодой учёный. – 2022. – № 38 (433). – С. 87–89.

5. Информационно-коммуникационные технологии обеспечения безопасности жизнедеятельности : монография / МЧС России [под общ. ред. П. А. Попова]. – М. : ФГУ ВНИИ ГОЧС (ФЦ), 2009. – 272 с.

6. Шарахутдинов Р. Б., Черкесов В. В. Анализ современных технологий и технических средств оповещения и информирования населения о чрезвычайных ситуациях // Пожарная и техносферная безопасность: проблемы и пути совершенствования. – 2020. – № 2 (6). – С. 485–489.

7. Цуриков А. Н., Ракитская Е. А. Мобильные приложения для оповещения об экстренных ситуациях // Научное обозрение. Технические науки. – 2018. – № 5. – С. 30–36.

8. Сулоева Н. В. Информационные технологии в вопросах обеспечения безопасности населения и территорий от чрезвычайных ситуаций // Научный Лидер. – 2022. – № 52 (97). – URL: https://scilead.ru/article/3594-informatsionnie-tekhnologii-v-voprosakh-obesp (дата обращения: 11.01.2026).

9. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. – Введ. 2016-01-01. – М. : Стандартинформ, 2015. – 28 с.

10. Соколов Ю. И. К вопросу организации оповещения населения при возникновении чрезвычайной ситуации // Проблемы анализа риска. – 2019. – № 1. – URL: https://cyberleninka.ru/article/n/k-voprosu-organizatsii-opovescheniya-naseleniya-pri-vozniknovenii-chrezvychaynoy-situatsii (дата обращения: 11.01.2026).

11. Леонова А. Н., Леонова Е. М. О комплексных системах экстренного оповещения населения // Столыпинский вестник. – 2023. – № 1. – URL: https://cyberleninka.ru/article/n/o-kompleksnyh-sistemah-ekstrennogo-opovescheniya-naseleniya (дата обращения: 11.01.2026).

12. Рыженко А. А., Рыженко Н. Ю., Эльтемерова О. В. Проблемы информирования и оповещения населения о чрезвычайных ситуациях // Технологии техносферной безопасности. – 2014. – № 2 (54). – 24 с.

References

1. On the Security of Critical Information Infrastructure of the Russian Federation: Federal Law No. 187-FZ of 26.07.2017 // Collection of Legislation of the Russian Federation. – 2017. – No. 31 (Part I). – Art. 4736.

2. On Approval of the Regulation on Public Warning Systems: Decree of the Government of the Russian Federation No. 1074 of 01.03.2019 (as amended on 23.10.2021) // Collection of Legislation of the Russian Federation. – 2019. – No. 10. – Art. 1028.

3. Requirements for Ensuring the Security of Significant Objects of Critical Information Infrastructure of the Russian Federation: Order of the FSTEC of Russia No. 239 of 25.12.2017. – Moscow, 2017.

4. Akhmedova Kh. M. Organizational and Legal Regulation of Public Information and Warning in the Event of a Threat or Occurrence of Natural or Man-Made Emergencies // Young Scientist. – 2022. – No. 38 (433). – P. 87–89.

5. Information and Communication Technologies for Life Safety: Monograph / EMERCOM of Russia [under the general editorship of P. A. Popov]. – Moscow: FGU VNII GOChS (FTs), 2009. – 272 p.

6. Sharakhutdinov R. B., Cherkesov V. V. Analysis of Modern Technologies and Technical Means of Public Warning and Notification about Emergencies // Fire and Technosphere Safety: Problems and Ways of Improvement. – 2020. – No. 2 (6). – P. 485–489.

7. Tsurikov A. N., Rakitskaya E. A. Mobile Applications for Emergency Notification // Scientific Review. Technical Sciences. – 2018. – No. 5. – P. 30–36.

8. Suloeva N. V. Information Technologies in Matters of Ensuring the Safety of the Population and Territories from Emergencies // Scientific Leader. – 2022. – No. 52 (97). – URL: https://scilead.ru/article/3594-informatsionnie-tekhnologii-v-voprosakh-obesp (accessed: 11.01.2026).

9. GOST R 34.12-2015. Information Technology. Cryptographic Protection of Information. Block Ciphers. – Introduced 2016-01-01. – Moscow: Standartinform, 2015. – 28 p.

10. Sokolov Yu. I. On the Issue of Organizing Public Warning in the Event of an Emergency // Risk Analysis Problems. – 2019. – No. 1. – URL: https://cyberleninka.ru/article/n/k-voprosu-organizatsii-opovescheniya-naseleniya-pri-vozniknovenii-chrezvychaynoy-situatsii (accessed: 11.01.2026).

11. Leonova A. N., Leonova E. M. On Integrated Emergency Public Warning Systems // Stolypin Bulletin. – 2023. – No. 1. – URL: https://cyberleninka.ru/article/n/o-kompleksnyh-sistemah-ekstrennogo-opovescheniya-naseleniya (accessed: 11.01.2026).

12. Ryzhenko A. A., Ryzhenko N. Yu., Eltemerova O. V. Problems of Public Information and Warning about Emergencies // Technologies of Technosphere Safety. – 2014. – No. 2 (54). – 24 p.