УДК: 004.056.53

МОДЕЛЬ ПРОЦЕССА АНАЛИЗА СЛУЖЕБНОГО ТРАФИКА ПРИ УПРАВЛЕНИИ БЕЗОПАСНОСТЬЮ ИНФОРМАЦИОННОЙ СЕТИ

SERVICE TRAFFIC ANALYSIS PROCESS MODEL FOR INFORMATION NETWORK SECURITY MANAGEMENT

М.А. Сорокин, А.А. Курило, канд. техн. наук П.И. Кузин

M.A. Sorokin, A.A. Kurilo, PhD P.I. Kuzin

ВАС им. С.М. Буденного

В статье предложена модель процесса анализа служебного трафика при управлении безопасностью информационной сети, которая необходима для анализа служебного трафика, так как он является источником информации о сети, её структуре, а также о характере ее функционирования. Процесс управления информационной безопасностью информационных систем должен получать информацию о текущем состоянии путем анализа цифрового потока соединения. Для обеспечения требуемой достоверности целесообразно учитывать свойства структуры цифрового потока, передаваемого в канале связи. Представленная модель позволит обеспечить необходимый уровень защищенности информационных систем, повысить эффективность сбора трафика за счет использования фильтров для пакетов, поддерживать работоспособность сети.
Ключевые слова: сетевой контроль, служебный трафик, кибербезоопасность, информационно-вычислительная сеть, цифровой поток, SIEM система.

The article proposes a model of the process of analyzing service traffic in the management of information network security, which is necessary for the analysis of service traffic, since it is a source of information about the network, its structure, as well as the nature of its functioning. The information security management process of information systems should obtain information about the current state by analyzing the digital flow of the connection. To ensure the required reliability, it is advisable to take into account the properties of the structure of the digital stream transmitted in the communication channel. The presented model will provide the necessary level of security of information systems, increase the efficiency of traffic collection, through the use of filters for packets, and maintain the network performance.
Keywords: network control, service traffic, cybersecurity, information and computing network, digital stream, SIEM system.

В настоящее время наблюдается рост количества и развитие информационных систем (ИС) в киберпространстве (КП). Для передачи пользовательских данных в них применяются различные протоколы, использование которых сопровождается служебной информацией.

ИС могут являться объектом воздействия кибератак (КА). Проблема обеспечения кибербезопасности (КБ) инфраструктуры стала одной из наиболее актуальных [1, 2]. Это стимулирует разработчиков систем безопасности охватывать максимально возможный спектр как источников

исходной информации для анализа состояния безопасности, так и источников индикаторов компрометации, профилей и сигнатур известных киберугроз [3, 4, 13–15].

Анализ цифровых потоков (ЦП) в ИС позволяет сделать вывод о том, что служебная информация может являться источником информации как о самой сети и её элементах, так и о характере её функционирования.

При осуществлении сетевого контроля особое внимание уделяется анализу служебного трафика, так как при анализе служебной информации потенциальный нарушитель может получить сведения о потенциальных объектах вторжения. Следовательно при сетевом контроле необходимо выявлять уязвимости служебной информации.

В процессе организации КБ при сетевом контроле необходимо распознать подготовку и реализацию КА в процессах сбора, хранения, обработки и передачи информации при попытках нарушителя воздействовать на инфраструктуру организации, выводя её из строя или снижая её эффективность [5].

Анализ служебной информации при сетевом контроле позволяет:

Во-первых, изучить логику работы, распределенной ИС, то есть получить взаимно однозначное соответствие событий, происходящих в системе, и команд, пересылаемых друг другу ее объектами, в момент появления этих событий (если проводить дальнейшую аналогию с инструментарием хакера, то анализ трафика в этом случае заменяет и трассировщик). Это достигается путем перехвата и анализа пакетов обмена на канальном уровне. Знание логики работы распределенной ИС позволяет на практике моделировать и осуществлять типовые удаленные атаки, рассмотренные в следующих пунктах на примере конкретных распределенных ИС;

Во-вторых, анализ сетевого трафика позволяет перехватить поток данных, которыми обмениваются объекты распределенной ИС. Удаленная атака данного типа заключается в получении на удаленном объекте несанкционированного доступа к информации, которой обмениваются два сетевых абонента. При этом отсутствует возможность модификации трафика и сам анализ возможен только внутри одного сегмента сети. Примером перехваченной при помощи данной типовой удаленной атаки информации могут служить имя и пароль пользователя, пересылаемые в незашифрованном виде по сети.

Определено противоречие заключающееся в том, что, с одной стороны, возможности по формированию и реализации КА на основе учета данных служебной информации значительно увеличились, а, с другой стороны, современные методы КБ оказываются не эффективными из-за недостаточной информированности о воздействиях на служебный трафик.

В работе [6, 15] рассматривается подход к разработке и использованию систем КБ, основанный на выделении интеллектуальной составляющей над традиционными способами защиты и построении единой унифицированной среды для создания и поддержки функционирования систем защиты. Однако не рассмотрены вопросы моделирования обнаружения аномальных отклонений, распознавания вторжений при сетевом контроле служебной информации и прогнозирования состояния защиты ИС. В работе [7] недостаточно внимания уделено анализу динамики действий нарушителя, которые включают сценарии внешних и внутренних вторжений. В работах анализируются частные показатели, и не учитываются особенности вторжений и воздействие нарушителей на служебный трафик. В действительности, не стоит пренебрегать тем фактом, что злоумышленники ежедневно находят новые способы обхода системы защиты информации (СЗИ), обнаруживают новые уязвимости в программах и протоколах.

Рассмотренные подходы и методы несомненно позволят выполнить поведенческий анализ пользователей, детектировать большинство известных атак, обнаружить ошибки в конфигурировании и функционировании оборудования и програмного обеспечения (ПО), но не позволят обнаружить технологические сбои или некорректную работу устройств канального и сетевого уровней (коммутаторов, маршрутизаторов, МСЭ), определить некорректное межсетевое взаимодействие, выполнить корреляцию этих событий с трафиком пользователей. Указанная проблема стала следствием эволюционного разделения сфер полномочий и ответственности администраторов сетевого оборудования и систем, и администраторов систем безопасности. Протоколы, не переносящие непосредственно

пользовательские данные, к сожалению, редко становятся объектом внимания ИС, но содержащаяся в них информация активно используется администраторами сетей. Таким образом, задача моделирования процесса анализа трафика служебной информации при осуществлении сетевого контроля является актуальной.

Цель — обеспечить достоверность определения зависимости показателя процесса анализа служебного трафика от внутренних и внешних параметров.

Задача — смоделировать процесс анализа служебного трафика при сетевом контроле безопасности информации.

Решение задачи заключается в анализе динамики действий нарушителя, обработке, определении уязвимостей системы защиты информации, уязвимостей служебных протоколов, а также выявлении аномалий в служебном трафике. При исследовании способов защиты было установлено, что наиболее подходящим решением для анализа событий безопасности являются SIEM-системы. Результаты анализа промышленных SIEM систем позволяют сделать вывод о том, что большинство из них поддерживают ограниченный набор протоколов получения исходной информации, и большая часть из них не имеют возможности интеграции со сторонними базами индикаторов компрометации. Таким образом, большая часть служебных протоколов канального и сетевого уровней остаются за пределами внимания этих систем.

Рассматривается структура ИВС, состоящая из следующих элементов (рис. 1).

Она включает в себя сетевые устройства, такие как маршрутизаторы и коммутаторы, главной задачей которых является обеспечение обмена данными между различными сегментами ИВС.

Демилитаризованная зона (ДЗ). Участок ИВС, находящийся на ее границе и соединяющийся с сетью Интернет через пограничный маршрутизатор. В этом участке ИВС располагаются службы, которые должны быть доступны пользователям внешней сети, такие как web-сервер, прокси-сервер и другие, а также, модуль сбора и анализа трафика, рис. 1.

Серверная ферма. Здесь располагаются серверы, обеспечивающие работу различных служб,

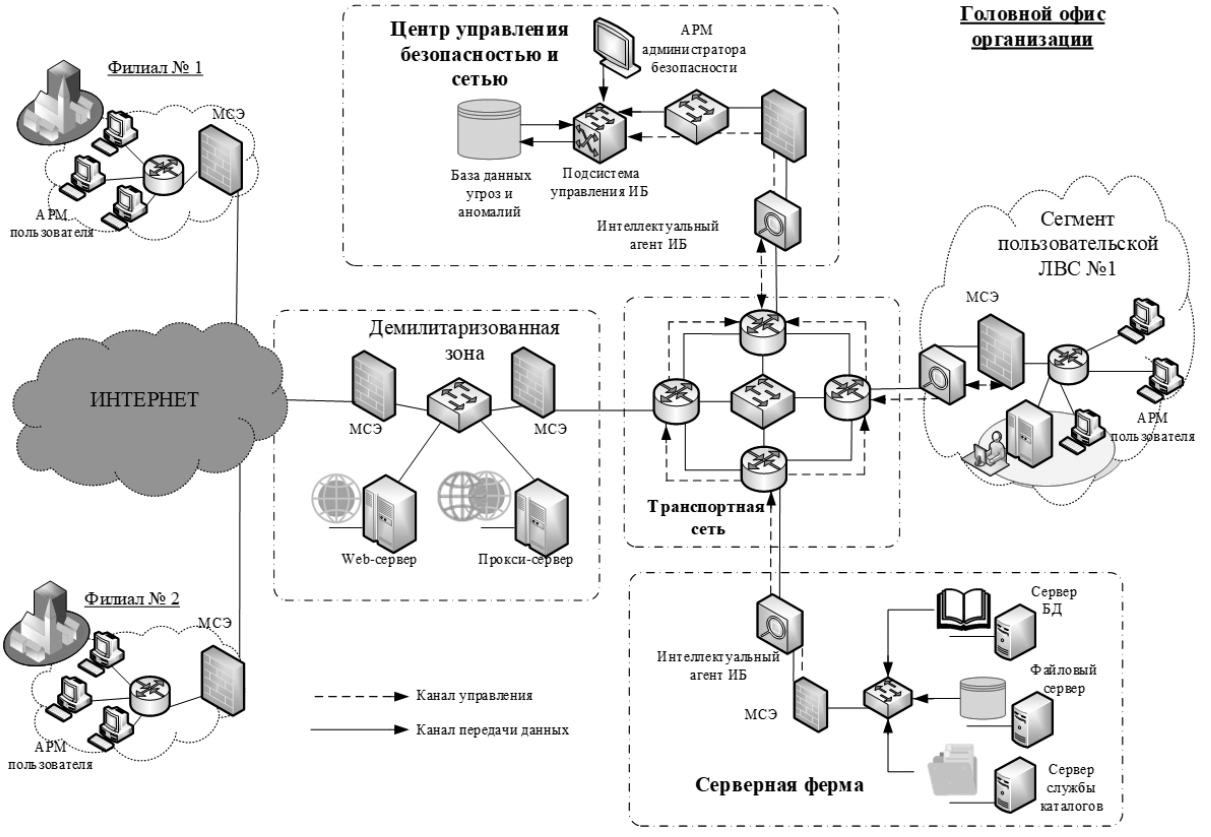

Рис. 1. Структурная схема рассматриваемой информационно-вычислительной сети

используемых внутри ИВС: файловый сервер, сервер баз данных, сервер службы каталогов и другие, рис. 1.

Центр управления безопасностью и сетью, задачей которого является контроль уязвимостей узлов сети и управление работой используемых СЗИ, рис. 1.

Пользовательская локальная вычислительная сеть (ЛВС), состоящая из рабочих мест пользователей, сетевых принтеров, телефонов и других устройств. Таких сетей может быть несколько, и они могут быть разделены по подразделениям или по другому принципу, предложенному администратором сети, рис. 1.

Цифровой поток входящий и исходящий из сети Интернет вначале проходит предварительную фильтрацию межсетевым экраном, после чего анализируется на предмет наличия атак. Затем поток перенаправляется на сервер, использующим библиотеку *libcap*, модуль *tcpdump* и модуль анализа пользовательского трафика *Snort*. Для этого на вход выделенного сетевого интерфейса, настроенного в режиме неразборчивой обработки пакетов, подается поток данных *span*-портов коммутаторов с использованием функции «зеркалирования» трафика от определённого *VLAN* или группы *VLAN*.

Большая часть существующих служебных протоколов используется для проведения атак типа «отказ в обслуживании» (*DNS, NTP, GRE, ICMP, xSTP, IGMP*), внедрения ложных объектов сети и перенаправления трафика (*ARP, OSPF, RIP, DNS, DHCP, DNS*), несанкционированного доступа к технологической информации (*CDP, LLDP, VTP, SNMP*), создания скрытых каналов связи (*ICMP, DNS*).

Детальный анализ информации в сообщениях служебных протоколов и ее корреляция с основным набором информации по событиям позволит не только увеличить достоверность выявления аномалий и вредоносного воздействия, но и реализовать дополнительные механизмы контроля состояния и безопасности телекоммуникационной сети и информационных систем [8, 11, 12].

Разделение трафика на пользовательский и служебный происходит на этапе его первичной обработки из *PCAP* файлов. В качестве критерия используется информация из полей *EtherType*, *SSAP, DSAP* в зависимости от типа *Ethernet*-кадра и поля «*Protocol*» заголовков *IP*-пакетов. Происходит детектирование аномального пользовательского и служебного трафика. Сгенерированные *IDS/IPS* системой *Snort* журналы уведомлений обнаружения аномального трафика отправляются в модуль анализа и корреляции. База знаний *SIEM* системы дополнительно обогащается информацией, позволяющей определить состояние телекоммуникационной инфраструктуры, корректность функционирования и использования служебных протоколов, наличие аномальных отклонений и выявить источники угрозы и несанкционированные каналы передачи информации. Разработана общая структура процесса анализа служебного трафика при сетевом контроле (рис. 2).

Процесс управления информационной безопасностью (ИБ) ИС должен получать информацию о текущем состоянии путем анализа ЦП соединения [9]. Для обеспечения требуемой достоверности целесообразно учитывать свойства структуры ЦП, передаваемого в канале связи. Цифровой поток (N) соединения ИС есть определенная на периоде существования соединения алгебраическая система:

$$A = \langle S, \{\oplus\}, \{R\} \rangle, \qquad (1)$$

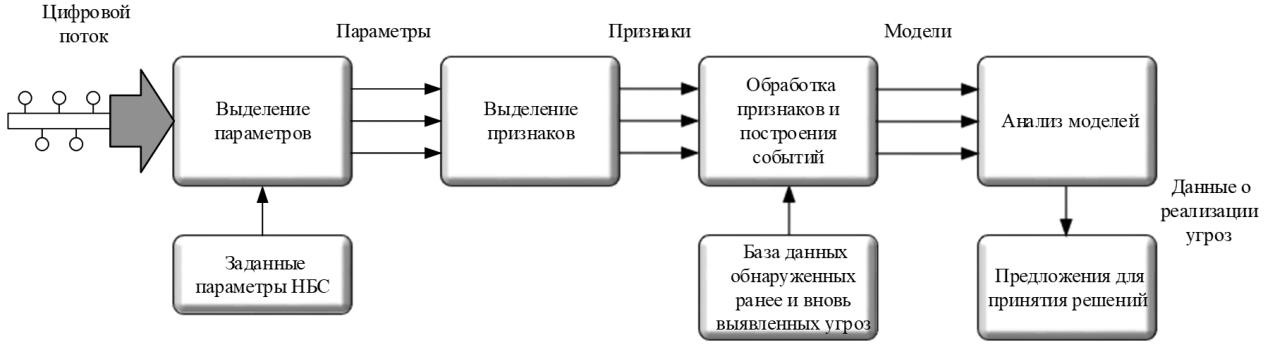

Рис. 2. Структура процесса анализа служебного трафика при сетевом контроле

где S — множество структурных элементов соединения (N) уровня эталонной модели взаимодействия открытых систем;

$\oplus$ — операция конкатенации на множестве структурных элементов;

R — бинарное отношение на множестве структурных элементов в (N) — цифрового потока соединения (ЦПС).

Структура ЦП (N)-соединения ИС, описываемого алгеброй вида (1), есть отношение строгого порядка, определенное на множестве структурных элементов (СЭ) и существующее на интервале, равном длительности существования соединения:

$$R = \{"(s_i, s_j, s_k)S, s_iRs_js_jRs_i, ij, ..., ..., s_iRs_js_jRs_ks_iRs_k, i < j < k\}, \quad (2)$$

где s_i, s_j, s_k — СЭ ИС.

Многие (N) протоколы ИС допускают конечное множество вариантов кодирования полей блока данных протокола и порядка следования (N) блоков передачи данных друг за другом в ходе сеанса обмена информацией в зависимости от различных факторов: состояния физического канала связи, протяженности и пропускной способности линии связи, параметров оконечного оборудования, используемого (N-1) протокола и др. В этом случае существует континуум $R(N)=\{R(N)_i\}$, каждый элемент которого соответствует конкретному режиму (N) протокола [10]. Процесс обмена данными и сигналами управления на (N) уровне (N=2...7) ИС может быть описан ЦП соответствующих соединений между (N) объектами сети с помощью алгебры вида:

$$A_{(N)} = \left\langle S_{(N)}, \{Å\}, \left\{R_{(N)}\right\}\right\rangle.$$

Размещение структурных элементов (N) ЦПС адекватно описывается бинарными отношениями строгого порядка вида (2).

Это утверждение справедливо как по отношению к последовательности передачи различных (N) блока данных протокола (БДП) в ходе сеанса обмена данными, так и к структуре самих (N) БДП.

Иерархическая протокольная структура ЦП ИС может быть представлена алгеброй вида $A \le S$, $\{Å\}$, $\{R\}$, где множество БДП каждого (N) протокола является подмножеством СЭ БДП (N-1) протокола:

$$A_{(N)} = \left\langle S_{(N)-\text{БДП}}, \{Å\}, \left\{R_{(N)}\right\}\right\rangle;$$

$$A_{(N)-\text{БДС}} = \left\langle S_{(N-1)-\text{БДП}}, \{Å\}, \{R_{(N-1)-\text{БДС}}\}\right\rangle;$$

$$A_{(N-1)} = \left\langle S_{(N-1)-\text{БДП}}, \{Å\}, \left\{R_{(N-1)}\right\}\right\rangle \text{ и т.д.}$$

Выражения представляют собой не что иное, как модель иерархии логических соединений в сквозном физическом канале ИС между двумя оконечными системами. Для моделирования суммарного трафика необходимо рассматривать упорядоченное множество пар (l, k) оконечных систем ИС. Объединение алгебр всех ЦПС (каждая из которых определяется на периоде существования (N) соединений данного сеанса обмена данными) на множестве каналов образуют модель трафика ИС (алгебру трафика сети A_{TC}):

$$A_{TC} = \grave{E}A_i\left(T_j\right)_{(l,k)},$$

где $A_i(T_j)_{(l,k)}$ — алгебра ЦПС i-го канала на периоде T_j существования j-го логического соединения между l-й и k-й оконечными системами ИС.

Таким образом, процесс анализа ЦП соединения ИС при управлении КБ учитывает свойства структуры ЦП, передаваемого в канале связи. Положительный эффект представляется получением возможности моделирования функционально-логической архитектуры ИС по отображениям на ЦП логических соединений в физических каналах связи, иерархическую взаимосвязь протоколов, что позволяет указывать местоположение и взаимосвязи структурных элементов ЦПС-носителей параметров нарушений, управляющей информации и данных пользователей.

Практическая значимость заключается в том, что предложенная модель процесса анализа служебного трафика позволит обеспечить необходимый уровень защищенности ИС, повысить эффективность сбора трафика, за счет использования фильтров для пакетов, поддерживать работоспособность сети. Определена группа параметров, необходимых для анализа трафика в ИС при контроле потоков служеб-

ных данных, определены критерии его классификации для последующего анализа при формировании событий КБ. Результаты станут основой для дальнейшей разработки модулей формирования событий КБ с учетом в корреляционных зависимостях информации служебных протоколов.

Литература

1. Шевченко А.А., Яцкин А.Д. и др. Метод управления безопасностью информационно-вычислительных сетей на основе выделенного сервера с контейнерной виртуализацией // Информационные системы и технологии. 2017. № 4 (102) С. 116–126.

2. Кузнецов И.А., Шевченко А.А. и др. Способ многофакторного управления безопасностью информационно-телекоммуникационной сети системы менеджмента качества предприятий интегрированных структур. — М: Вопросы радиоэлектроники. 2016. № 6. С. 23–28.

3. Коршунов Г.И., Шевченко А.А., Малышев Б.Ю. и др. Метод адаптивного управления защитой информационно-вычислительных сетей на основе анализа динамики действий нарушителя // Информационно-управляющие системы. 2018. № 4. С. 61–72. doi:10.31799/1684-8853-2018-4-61-72.

4. Липатников В.А., Шевченко А.А. Способ контроля уязвимостей при масштабировании автоматизированной системы менеджмента предприятия интегрированной структуры // Информационные системы и технологии. 2016. № 2 (94). С. 128–140.

5. Кузнецов А.В., Муравьева Д.С. Создание систем управления событиями и инцидентами ИБ (SIEM) // Журнал «Information Security». 2012. № 3. С. 28–29.

6. Кузин П.И., Рабин А.В. и др. Передачи сигналов в каналах связи с замираниями Накагами // Успехи современной радиоэлектроники. — М.: «Издательство Радиотехника». 2019. № 11. С. 71–78.

7. Rabin A.V., Lipatnikov V.A., Kuzin P.I. Signal protection methods in channels with Nakagami fading // «International Conference on Metrological Support of Innovative Technologies» (ICMSIT-2020). — Krasnoyarsk: Journal of Physics: Conference Series.

8. Кузин П.И., Липатников В.А. Метод повышения оперативности смены параметров адаптации, при приеме информации в системах радиосвязи КВ — УКВ диапазонов // Научный журнал «Автоматизация процессов управления». 2016. № 4 (46). С.18–22.

9. Кузин П.И., Рабин А.В. и др. Метод повышения надежности помехозащищенности при приеме информации в системах радиосвязи СВЧ- и КВЧ-диапазонов Радиотехника. 2020. Т. 84. № 8 (16). С. 5–12.

10. Lipatnikov V.A., Kuzin P.I., Rabin A.V. The method of increasing the reliability of noise immunity when receiving information in radio communication systems of the shf and ehf ranges. В сборнике: Journal of Physics: Conference Series. — Krasnoyarsk Science and Technology City Hall of the Russian Union of Scientific and Engineering Associations. — Krasnoyarsk. Russian Federation. 2020. С. 52100.

11. Болюбаш О.О. Алгоритм сбора, обработки и передачи информации о состоянии сети передачи данных. Информационные технологии: наука, техника, технология, образование, здоровье. Материалы XI международной НПК. — НТУ «XIII». 2003. 45 с.

12. Кочегаров В.А. Проектирование систем распределения информации. Марковские и немарковские модели. — М.: Радио и связь. 1991. 214 с.

13. Стародубцев Ю. И. Способ обнаружения источника сетевых атак на автоматизированные системы / Ю.И. Стародубцев, В.Г. Федоров // Журнал «Проблемы экономики и управления в торговле и промышленности». № 1. 2016. 87 с.

14. Макаренко С.И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки. Монография. — СПб.: Наукоемкие технологии. 2020. 130 с.

15. Костарев С.В., Карганов В.В., Липатников В.А. Технологии защиты информации в условиях кибернетического противоборства: Науч. монография / Под общ. ред. В.А. Липатникова. — СПб: ВАС. 2020. 716 с.: ил. ISBN 978-5-91690-044-6.

References

1. Shevchenko A.A., Yatskin A.D. Method of security management of information and computing

networks based on a dedicated server with container virtualization // Information systems and Technologies. 2017. № 4 (102) P. 116–126.

2. Kuznetsov I.A., Shevchenko A.A. et al. The method of multifactorial security management of the information and telecommunications network of the quality management system of enterprises of integrated structures. — M.: Questions of radio Electronics. 2016. № 6. P. 23–28.

3. Korshunov G.I., Shevchenko A.A., Malyshev B.Yu. et al. Method of adaptive management of information and computer network protection based on the analysis of the dynamics of the violator's actions. 2018. № 4. P. 61–72. doi:10.31799/1684-8853-2018-4-61-72.

4. Lipatnikov V.A., Shevchenko A.A. Method of vulnerability control when scaling the automated management system of an integrated structure enterprise // Information Systems and Technologies. 2016. № 2 (94). P. 128–140.

5. Kuznetsov A.V., Murav'eva D.S. Creation of information security event and incident management systems (SIEM) // Journal «Information Security». 2012. № 3. P. 28–29.

6. Kuzin P.I., Rabin A.V. et al. Transmission of signals in communication channels with Nakagami fades // Uspekhi sovremennoy radioelectroniki. — M.: «Publishing House Radiotekhnika». 2019. № 11. P. 71–78.

7. Rabin A.V., Lipatnikov V.A., Kuzin P.I. Methods of signal protection in channels with Nakagami fading // «International Conference on Metrological Support of Innovative Technologies» (ICMSIT-2020). — Krasnoyarsk: journal of physics: conference Series.

8. Kuzin P.I., Lipatnikov V.A. A method for increasing the efficiency of changing adaptation parameters when receiving information in HF — VHF radio communication systems. // Scientific Journal «Automation of management processes». 2016. № 4 (46). P. 18–22.

9. Kuzin P.I., Rabin A.V. et al. Method of increasing the reliability of noise immunity when receiving information in radio communication systems of the microwave and EHF bands Radio engineering. 2020. Vol. 84. № 8 (16). P. 5–12.

10. Lipatnikov V.A., Kuzin P.I., Rabin A.V. Method for improving the reliability of noise immunity when receiving information in radio communication systems of microwave and EHF bands. Krasnoyarsk Scientific and Technical City Hall of the Russian Union of Scientific and Engineering Associations. — Krasnoyarsk. Russian Federation. 2020. P. 52100.

11. Bolyubash O.O. Algorithm for collecting, processing and transmitting information about the state of the data transmission network. Information technologies: science, technology, technology, education, health. Materials of the XI international NPC. — NTU «XIII». 2003. 45 p.

12. Kochegarov V.A. Design of information distribution systems. Markov and non-Markov models. — Moscow: Radio and communications. 1991. 214 p.

13. Starodubtsev Yu.I. Method of detecting the source of network attacks on automated systems / Yu.I. Starodubtsev, V.G Fedorov // Journal «Problems of Economics and Management in Trade and Industry». № 1. 2016. 87 p.

14. Makarenko S.I. Communication system models under conditions of deliberate destabilizing influences and reconnaissance. Monograph. —SPb: Science-intensive technologies 2020. 130 p.

15. Kostarev S.V., Karganov V.V., Lipatnikov V.A. Technologies of information protection in conditions of cybernetic confrontation: Scientific. monograph / Under total. ed. V.A. Lipatnikova. — SPb: VAS. 2020. 716 p.: ill. ISBN 978-5-91690-044-6.