**DOI 10.36622/VSTU.2022.25.2.012**
**УДК 004.72**

# ПОДХОД К ОРГАНИЗАЦИИ ЕДИНОГО ЦЕНТРА МОНИТОРИНГА С СОХРАНЕНИЕМ СВОЙСТВА ФИЗИЧЕСКОЙ ИЗОЛЯЦИИ СЕГМЕНТОВ ДЛЯ ИЗНАЧАЛЬНО НЕПЕРЕСЕКАЮЩИХСЯ СЕТЕЙ

**Ю.Ю. Громов, П.И. Карасев, Ю.Д. Забалуева, Д.Д. Маланьин**

На сегодняшний день задача контроля функционирования инфраструктуры является актуальной для многих организаций. Осуществление централизованного контроля позволяет улучшить показатели реагирования на инциденты и снизить потенциальный ущерб. Задача сохранения безопасности инфраструктуры является важным аспектом, которых необходимо учитывать при внедрении новых элементов в функционирующую информационную систему. В наше время эта тема имеет большую значимость в силу постоянно развивающихся способов атак на инфраструктуру организации. В данной статье описаны методы сохранения уровня безопасности инфраструктуры на прежнем уровне после внедрения единого центра мониторинга, использование которого позволяет ускорить реагирование на инциденты.

Ключевые слова: информационная безопасность, система мониторинга, непересекающиеся сети, однонаправленный канал передачи.

В настоящее время все больше компаний стремятся уделять внимание безопасности своей инфраструктуры и обращаются к использованию сегментации сетей.

Оборудование, обеспечивающее функционирование отдельных сервисов, выносится в непересекающиеся сегменты или сети. Такой подход позволяет эффективно разграничить уровни доступа, обеспечить независимость групп оборудования и повысить отказоустойчивость сетевой инфраструктуры в целом. При правильной организации в каждом из сегментов налажена собственная система передачи траффика, и, в случае отказа оборудования в одном из сегментов, другие сервисы способны полноценно функционировать, обеспечивая работу компании и способствуя минимизации бизнес-ущерба.

Разделение бизнес-процессов и, соответственно, компонентов инфраструктуры рекомендовано в качестве одной из ключевых мер построения эффективной системы защиты компании [1].

Мониторинг состояния оборудования является одной из фундаментальных задач обеспечения непрерывного функционирования сервисов компании. Однако задача организации мониторинга распределенной инфраструктуры является нетривиальной и требует комплексного подхода при ее решении.

Обманчиво простым решением является создание системы мониторинга в каждом из отдельных сегментов. Однако, в случае такой организации мониторинга, сложность представляет индивидуальная проверка каждого из сегментов, в результате чего время реагирования на инциденты может возрастать.

Более эффективным решением представляется организация единого центра мониторинга (далее – ЕЦМ), куда будут передаваться данные из всех сегментов. Такой подход позволяет оценить общее состояние распределенной системы, используя агрегированные данные мониторинга, и обеспечить возможность оперативного реагирования на события информационной безопасности.

Одной из важных особенностей вышеописанного подхода к организации ЕЦМ является внесение избыточности относительно обрабатываемых данных мониторинга, тем самым, обеспечивая резервирование этих данных. Подход

обеспечивает возможность хранения данных мониторинга не только внутри сегмента серверного оборудования, но и внутри сегмента мониторинга [2].

В случае несанкционированных действий внутри сегмента оборудования с последующим удалением соответствующих записей о них, информация об активности нарушителя не исчезнет бесследно, а сохранится и будет доступна персоналу ЕЦМ.

Стремление к объединению данных, получаемых от распределенных систем, наблюдается на рынке и постепенно приобретает все большую популярность среди крупных территориально-распределенных организаций. Так, например, по подобному пути пошла компания Huawei. На своей конференции «Цифровое сообщество 2021» компания продемонстрировала разработку платформы, позволяющей объединить системы географически распределенных зданий в единую информационную систему [3].

Опишем реализацию предложенного выше подхода с ЕЦМ на основе уже существующей топологии, включающей в себя некоторое количество физически изолированных относительно друг друга сетей. Внутри каждого из сегментов размещено серверное оборудование и реализован сбор данных мониторинга его состояния.

Сбор и обработка данных осуществляются на основе протокола Simple Network Management Protocol (SNMP). Принцип работы данного протокола заключается в использовании так называемого центра мониторинга – административного компьютера, далее именуемого Менеджером. На конечных точках, от которого требуется получить информацию, размещены специальные программные модули – Агенты. Типовая схема протокола представлена на рис. 1.

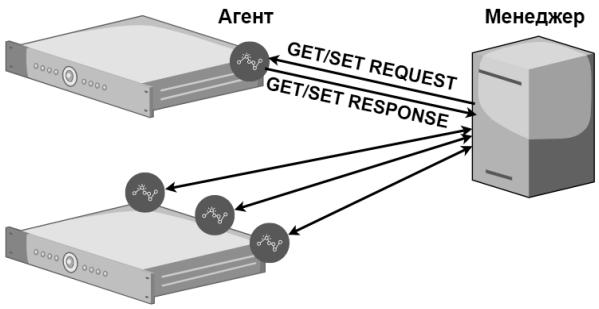



Рис. 1. Типовая схема работы протокола SNMP

Внутри сегмента взаимодействие Менеджера и Агентов осуществляется в штатном режиме, предусмотренном классической реализацией протокола. Для получения информации о состоянии оборудования из внешней сети необходимо обратиться к Менеджеру.

Изначальная топология сетевой инфраструктуры представлена на рис. 2.

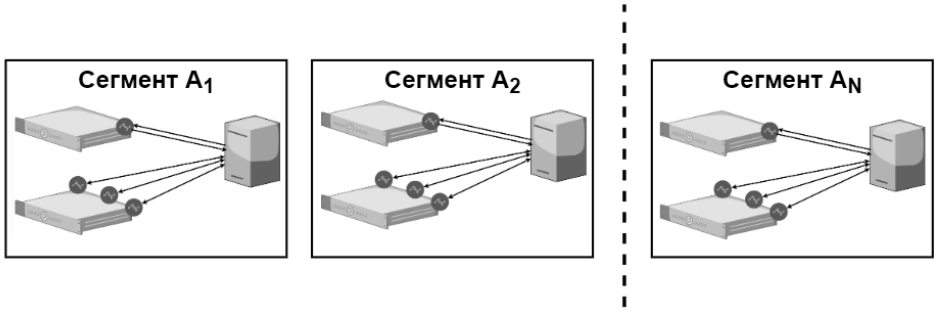



Рис. 2. Изолированные сегменты оборудования

Добавим сегмент мониторинга, в который будут передаваться данные от каждого из Менеджеров во всех сегментах. Персонал ЕЦМ таким образом получает возможность осуществлять централизованный контроль за состоянием оборудования во всех сетях. В приведенной схеме пропадает необходимость индивидуальной проверки каждого Менеджера, что, в свою очередь, приводит к ускорению процедуры реагирования на оповещения о событиях безопасности и упрощает оценку общего состояния инфраструктуры организации. Топология приобретает следующий вид (рис. 3):

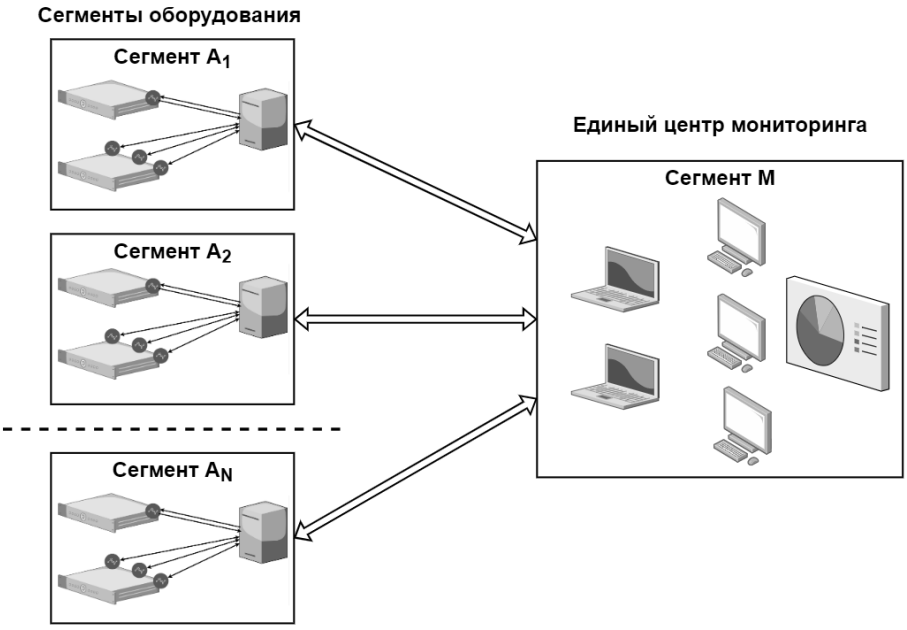



Рис. 3. Проблемы безопасности в новой топологии

Однако на данном этапе решение обладает рядом недостатков, главным из которых является то, что после добавления сегмента мониторинга уровень безопасности сетевой инфраструктуры существенно упал. Падение уровня безопасности произошло вследствие того, что ранее физически обособленные сегменты стали связанными, что представляет из себя серьёзную угрозу безопасности, а также нарушает изначальную концепцию о непересечении сетей в топологии, приведенной на рис. 2. Изначально злоумышленник даже в случае успешного проникновения и повышения привилегий был ограничен одним изолированным сегментом. После внесения изменений в топологию появилась угроза распространения в другие элементы сетевой инфраструктуры. В подобном аспекте канал передачи данных в сегмент мониторинга представляет из себя потенциальный канал утечки и компрометации информации [4].

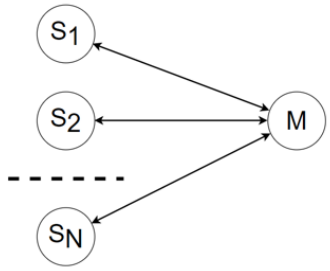
Для сохранения уровня безопасности системы на изначальном уровне требуется сохранить свойство физической изоляции сегментов. Сперва опишем предлагаемое решение поставленной проблемы на концептуальном уровне.

Представим задачу в виде математической абстракции. Вершины $S_1$, $S_2$., ..., $S_N$ обозначают *i*-й сегмент оборудования соответственно. Будем именовать эти вершины основными. Отметим, что каждая вершина достижима из себя самой путем нулевой длины. Исходные данные поставленной задачи, представленные в виде графа, и матрица достижимости для него приведены на рис. 4.


| | $S_1$ | $S_2$ | ... | $S_N$ |
|---|---|---|---|---|
| $S_1$ | 1 | 0 | ... | 0 |
| $S_2$ | 0 | 1 | ... | 0 |
| ... | ... | ... | ... | ... |
| $S_N$ | 0 | 0 | ... | 1 |

Рис. 4. Исходные данные и начальная матрица достижимости

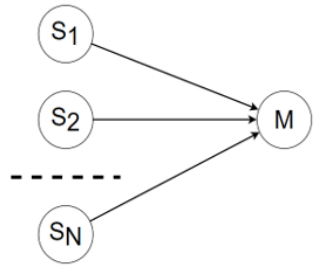
Внесем понятие вторичной вершины, добавленной для решения задачи. Вершина M является обозначением сегмента мониторинга. Целью является формирование маршрутов из сегмента оборудования в сегмент мониторинга, то есть маршрутов $S_1$–M, $S_2$–M, ..., $S_N$–M. После внесения изменений в систему и выделения дополнительный вершины структура претерпевает изменения. Взаимосвязь вершин и матрица достижимости представлены на рис. 5.




| | $S_1$ | $S_2$ | ... | $S_N$ | M |
|---|---|---|---|---|---|
| $S_1$ | 1 | 1 | ... | 1 | 1 |
| $S_2$ | 1 | 1 | ... | 1 | 1 |
| ... | ... | ... | ... | ... | ... |
| $S_N$ | 1 | 1 | ... | 1 | 1 |
| M | 1 | 1 | ... | 1 | 1 |

Рис. 5. Промежуточная схема и матрица достижимости для графа с двунаправленными связями

Между изначально независимыми вершинами $S_1$, $S_2$., ..., $S_N$ появились дополнительные двунаправленные связи. Наличие связей такого характера позволяет сформировать сложные маршруты из одной основной вершины в другую через вторичную. Чтобы исключить не соответствующие условию задачи маршруты, сделаем связи однонаправленными (рис. 6).




| | $S_1$ | $S_2$ | ... | $S_N$ | M |
|---|---|---|---|---|---|
| $S_1$ | 1 | 0 | ... | 0 | 1 |
| $S_2$ | 0 | 1 | ... | 0 | 1 |
| ... | ... | ... | ... | ... | ... |
| $S_N$ | 0 | 0 | ... | 1 | 1 |
| M | 0 | 0 | ... | 0 | 1 |

Рис. 6. Итоговая схема и финальная матрица достижимости для ориентированного графа

Данная модель является решением задачи, так как цель достигнута, и результат удовлетворяет начальным условиям.

Следующим этапом является реализация решения на уровне сетевой архитектуры. Среди способов обеспечения канала однонаправленной передачи можно выделить два основных подхода: логический и физический [5].

Одним из механизмов безопасности на логическом уровне является межсетевой экран. Современные межсетевые экраны способны осуществлять глубокий анализ трафика сразу на нескольких уровнях модели OSI. На рынке представлен широкий ряд межсетевых устройств от разных производителей, позволяющих посредством конфигурирования оборудования обеспечить блокировку трафика в одном из направлений. Данное решение обладает гибкостью за счет возможности настроек параметров устройства под нужды конкретной сети. Топология с использованием межсетевых экранов представлена на рис. 7.

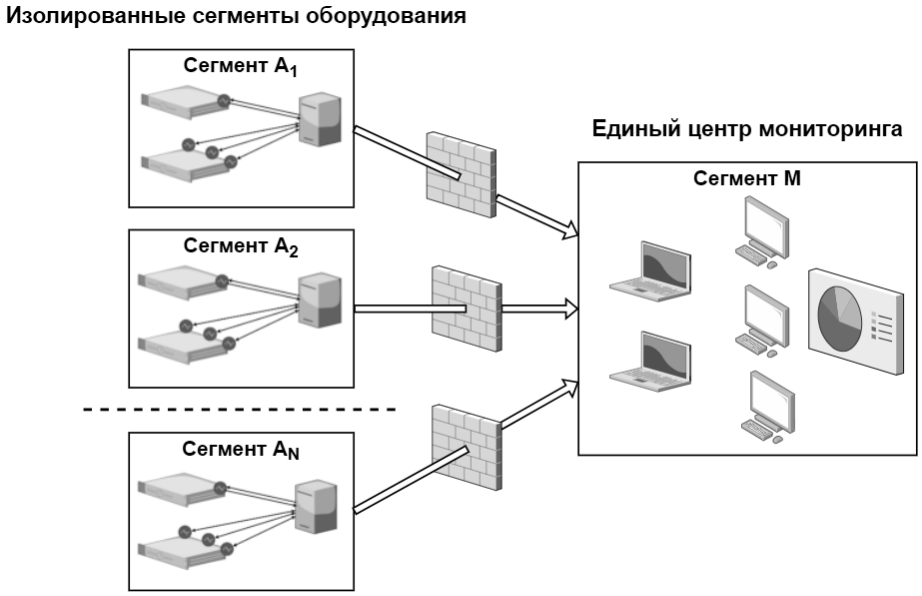



Рис. 7. Структура сети с использованием межсетевых экранов

Однако межсетевые экраны не могут реализовать гарантированное предотвращение утечек данных из сетевых сегментов в силу ряда недостатков, присущего данной технологии. Одной из распространенных причин компрометации межсетевых экранов является человеческий фактор, например, некорректные настройки правил межсетевого экранирования администратором.

Блокировка трафика межсетевым экраном осуществляется на основании формируемого правилами паттерна, из чего следует, что блокировку нельзя считать полной. Даже при корректных настройках злоумышленником после получения учетных данных администратора может быть изменена конфигурация устройства и спровоцирована угроза безопасности организации [6].

Еще более серьезным недостатком является использование программного обеспечения, что вносит вероятность наличия ошибок и формирует угрозу эксплуатации злоумышленником данных уязвимостей.

В качестве примера недостаточной надежности топологии на основе межсетевых экранов можно привести данные из отчета Positive Technologies «Итоги внешних пентестов – 2020». Экспертами компании в начале 2020 года были обнаружены две уязвимости нулевого дня в одной из моделей межсетевых экранов компании Cisco. Одним из последствий их эксплуатации было отключение ряда настроек и попадание злоумышленника во внутреннюю сеть [7].

Угроза, вносимая человеческим фактором, часто оказывает существенное влияние на безопасность сети. Распределение уровней риска ошибок конфигурации, обнаруженных экспертами Positive Technologies в ходе внешних пентестов за 2020-й год, представлено на рис. 8.

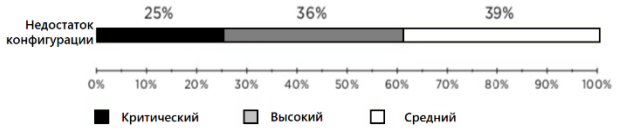



Рис. 8. Оценка опасности уязвимости «Недостаток конфигурации»

Таким образом, решение на основе межсетевых экранов обладает рядом потенциальных уязвимостей, возможность и опасность реализации которых подтверждены на практике.

Физически требуемый канал передачи может быть реализован на основе однонаправленного шлюза, также известного как Data Diode. Он представляет из себя устройство, на физическом уровне имеющее канал для передачи только в одном направлении и предназначенное для передачи информации между защищенным сегментом сети и менее защищенным/незащищенным.

Применительно к поставленной задаче топология с использованием канала на основе однонаправленного шлюза имеет следующий вид (рис. 9):

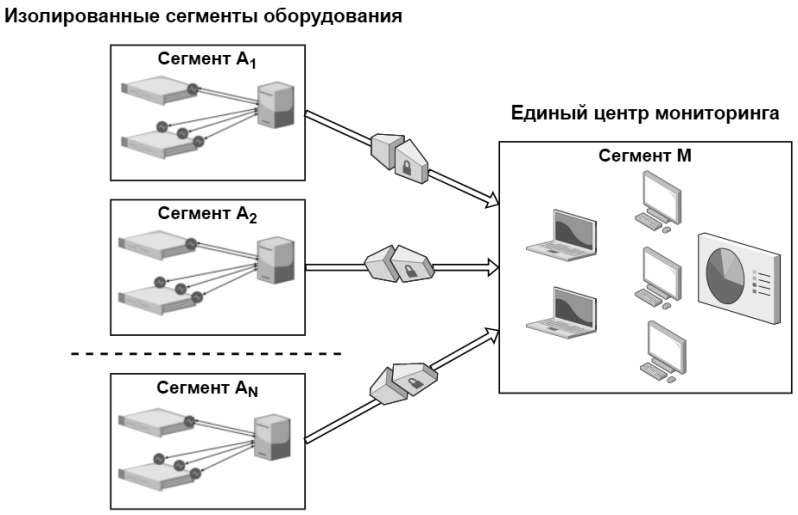



Рис. 9. Структура сети с использованием однонаправленного шлюза

Использование Data Diode полностью исключает возможность передачи трафика в обратную сторону. Решение на его основе лишено недостатков, присущих межсетевым экранам: канал формируется на аппаратном уровне. При нарушении целостности или его выходе из строя исчезает возможность использования канала передачи.

Недостатком данного решения может считаться его стоимость. Для организации полноценно работоспособного канала требуется не только аппаратная часть – однонаправленный шлюз – но и программное обеспечение, предназначенное для обработки данных, поступающих от протокола SNMP. Представленные на рынке решения могут оказаться достаточно затратными при большом объеме каналов мониторинга.

Однако в настоящее время ведутся исследования в области разработки более бюджетных решений. Примером может служить разработка программно-аппаратного комплекса для систем видеонаблюдения на основе технологии однонаправленной передачи, себестоимость которого значительно ниже рыночных аналогов [8].

Таким образом, были рассмотрены два подхода организации однонаправленного канала для системы мониторинга серверного оборудования. Обе реализации обеспечивают защищенность сегмента мониторинга от утечек информации и позволяют говорить о формировании однонаправленного канала передачи данных. Решения дают возможность реализовать сбор информации по отдельным каналам от нескольких сегментов и тем самым сформировать ЕЦМ с выполнением изначальных требований и сохранением физического непересечения изначально независимых сегментов. Однонаправленность трафика обеспечивает защищенность данных в сегменте мониторинга от утечек или внесения изменений путем удаления. Таким образом решается проблема сокрытия присутствия злоумышленника в случае, если им удаляются следы своего присутствия на Менеджере в сегменте оборудования.

На основе рассмотренных преимуществ и недостатков каждого из подходов можно сделать вывод, что уровни надежности предложенных решений различаются, так же, как и затраты на их внедрение. Выбор той или иной реализации зависит от ряда факторов, включающих в себя, но не ограничивающихся степенью критичности системы и выделенным бюджетом мероприятия.

Перспективным направлением является разработка решения на основе однонаправленного шлюза с ограниченным функционалом. Исключение Менеджера из сегмента мониторинга позволит напрямую передавать данные от Агентов в ситуационный центр. Однако, так как ряд используемых протоколом SNMP сообщений требует ответа для правильного функционирования протокола, таким образом может быть реализована передача только сообщений об ошибках – trap-сообщений [9].

Подобное решение проще в настройке. Оно может оказаться востребованным для инфраструктуры, где требуется обрабатывать ошибки, но отсутствует необходимость в отслеживании текущего состояния оборудования. Следует отметить, что подобному решению будет свойственно большое количество каналов передачи данных и/или отслеживание только отдельных агентов. Типовая схема представлена на рис. 10.

Альтернативным направлением дальнейшей работы можно поставить реализацию решения на основе однонаправленного шлюза, описанного в работе, посвященной разработке программно-аппаратного комплекса для систем видеонаблюдения [10]. Для осуществления этого требуется дальнейшая разработка программной реализации канала между Менеджером и сегментом мониторинга (рис. 11).

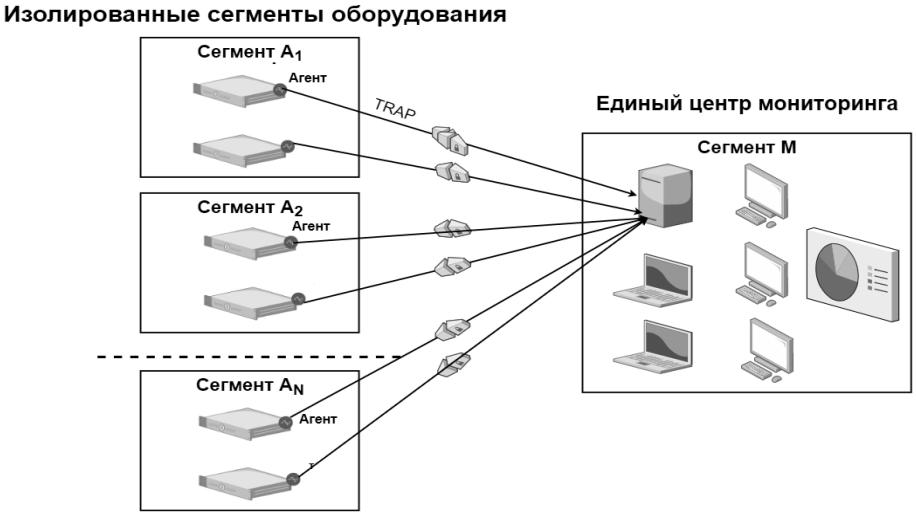



Рис. 10. Схема решения с ограниченным функционалом на основе однонаправленного шлюза

Протокол SNMP работает на основе UDP. Возможна разработка программного обеспечения, эмулирующего принимающее устройство и осуществляющего преобразование данных для передачи посредством UDP. Однонаправленный шлюз способен обеспечить передачу данных через указанный протокол. На принимающей стороне программное обеспечение осуществляет обратную операцию, данные в сегменте мониторинга доступны в изначальном формате.

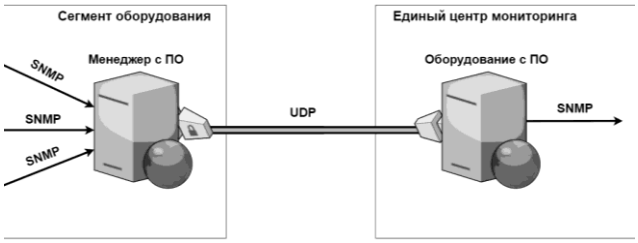



Рис. 11. Схема программно-аппаратного комплекса

## Список литературы

1. Positive Technologies: Бизнес под прицелом: анализируем сценарии атак. // URL: https://www.ptsecurity.com/ru-ru/research/analytics/pentests-2021-attack-scenarios/?sphrase_id=99203/ (дата обращения 27.03.2022).

2. Хабр: Распределенные ЦОД от провайдера: что и зачем // URL: https://habr.com/ru/company/ruvds/blog/412829/ (дата обращения 28.03.2022)

3. Huawei: Конференция Huawei Цифровое сообщество 2021 // URL: https://huawei.ru/events/hdcc2021/ (дата обращения 28.03.2022).

4. Актуальные киберугрозы: III квартал 2021 года: // Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q3/ (дата обращения: 28.03.2022).

5. Panopta: Agent vs. Agentless Monitoring: Which is best for your infrastructure? // URL: https://www.panopta.com/resources/agent-vs-agentless-monitoring/ (дата обращения 28.03.2022).

6. Денисов Д.В., Лихоносов А.Г. Интернет-курс «Основы аудита информационной безопасности»: // Megacampus. URL: http://www.e-biblio.ru/book/bib/01_informatika/audit_informac_bezopasnosty/up.html#_Toc256521632 (дата обращения: 24.03.2022).

7. Positive Technologies: Итоги внешних пентестов – 2020 // URL: https://www.ptsecurity.com/ru-ru/research/analytics/external-pentests-2020/?sphrase_id=99214/ (дата обращения 27.03.2022).

8. Idera: The truth about agent vs. agentless monitoring // URL: https://www.idera.com/~/media/Corporate/Files/WhitePapers/IderaWP_Agent_vs_Agentless_Monitoring.ashx/ (дата обращения 27.03.2022).

9. Гарда Технологии: Инциденты информационной безопасности. // URL: https://gardatech.ru/articles/smi/intsidenty-informatsionnoy-bezopasnosti-vyyavlenie-i-rassledovanie/ (дата обращения 27.03.2022).

10. Громов Ю.Ю. Размещение узлов сетевой информационной системы с комбинаторной топологией с целью повышения эффективности защиты информации в условиях неопределенности / Ю.Ю. Громов, Ю.В. Минин, С.А. Копылов // Информация и безопасность. 2019. Т. 22. Вып. 2. С. 272–279.

Тамбовский государственный технический университет
Tambov State Technical University

МИРЭА – Российский технологический университет
MIREA – Russian Technological University

Поступила в редакцию 5.05.2022

**Информация об авторах**

**Громов Юрий Юрьевич** – д-р техн. наук, профессор, Тамбовский государственный технический университет, e-mail: gromovtambov@yandex.ru

**Карасев Павел Игоревич** – канд. техн. наук, МИРЭА – Российский технологический университет, e-mail: karasev@mirea.ru

**Забалуева Юлия Дмитриевна** – студент, МИРЭА – Российский технологический университет, e-mail: uliya.zabalueva@mail.ru

**Маланьин Данила Дмитриевич** – аспирант, МИРЭА – Российский технологический университет, e-mail: mnac@comch.ru

## AN APPROACH TO ORGANIZING A SINGLE MONITORING CENTER WHILE MAINTAINING THE PROPERTY OF PHYSICAL ISOLATION OF SEGMENTS FOR INITIALLY NON-OVERLAPPING NETWORKS

**Y.Y. Gromov, P.I. Karasev, Y.D. Zabalueva, D.D. Malanin**

Today, the task of monitoring the functioning of the infrastructure is relevant for many organizations. Implementation of centralized control allows you to improve incident response rates and reduce potential damage. The task of maintaining infrastructure security is an important aspect that must be taken into account when introducing new elements into a functioning information system. In our time, this topic is of great importance due to the constantly evolving methods of attacks on the infrastructure of the organization. This article describes methods for maintaining the security level of the infrastructure at the same level after the implementation of a single monitoring center, the use of which allows you to accelerate incident response.

Keywords: information security, monitoring system, non-overlapping networks, unidirectional transmission channel.

Submitted 5.05.2022

**Information about the authors**

**Yurii Y. Gromov** – Dr. Sc. (Technical), Professor, Tambov State Technical University, e-mail: gromovtambov@yandex.ru

**Pavel I. Karasev**– Cand. Sc. (Technical), MIREA – Russian Technological University, e-mail: karasev@mirea.ru

**Yulia D. Zabalueva** – Student, MIREA – Russian Technological University, e-mail: uliya.zabalueva@mail.ru

**Danila D. Malanin** – Graduate Student, MIREA– Russian Technological University, e-mail: mnac@comch.ru