Эшелон
комплексная безопасность

АКЦИОНЕРНОЕ ОБЩЕСТВО
«НАУЧНО-ПРОИЗВОДСТВЕННОЕ ОБЪЕДИНЕНИЕ «ЭШЕЛОН»

107023, г. Москва, ул. Электрозаводская, д. 24, стр. 1, тел./факс: +7 (495) 223 23 92, 645 38 11, mail@npo-echelon.ru, www.npo-echelon.ru

Исх. № 133/1 от 3 февраля 2021 г.

Утверждаю
Генеральный директор
АО «НПО «Эшелон»
кандидат технических наук, доцент

В.Л.Цирлов

« 3 » февраля 2021 г.

ОТЗЫВ
на автореферат диссертации

Милославской Натальи Георгиевны «Построение центров управления сетевой безопасностью в информационно-телекоммуникационных сетях», представленной на соискание ученой степени доктора технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

I. Актуальность проблематики и темы диссертационного исследования

Актуальность работы объясняется потребностью разрешения проблемной ситуации, состоящей в противоречии между высоким уровнем неопределенности оценки предупреждения (фактически невозможностью прогнозирования) современных кибератак на ресурсы информационно-телекоммуникационных сетей (ИТКС) и собственно недостаточным уровнем развития теоретических исследований и разработанности методической базы превентивных действий и ситуационного управления уровнем информационной безопасности систем, в первую очередь основанной на современных приложениях технологий искусственного интеллекта.

Указанная проблематика, на наш взгляд, коррелируется с «Основными направлениями научных исследований в области обеспечения ИБ РФ» (Совет Безопасности Российской Федерации, 2017 г.) по п. 2.2.9.

Тема диссертации, направленность проведенных исследований и полученных результатов соответствуют Паспорту специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» по п. 1 и др.

II. Обоснованность научных положений, выводов и рекомендаций, сформулированных в диссертации, их достоверность и новизна

Судя по автореферату, в диссертационном исследовании автор, опираясь на проведенный анализ ЖЦ объектов ИТКС (и их СМИБ, и подсистем управления ИБ), нормативно-правой базы в части систем управления ИБ (и событий ИБ), построения центров мониторинга и ситуационных центров ИБ (включая центры СОПКА), таксономий и систематик информационной безопасности, техник и тактик кибератак и атрибуции кибергрупп, инструментальной базы контроля, мониторинга и управления сетевой безопасности, формальных моделей и методов управления безопасностью сетевых ресурсов на всех этапах ЖЦ, управления рисками, а также прикладных пакетов компьютерного моделирования (в том числе интеллектуального содержания), демонстрирует системность и комплексность своего подхода к постановке и разрешению научной проблемы.

Оригинальность работы состоит в том, что автор аргументировано предложил концептуальный (неформальный) подход к выбору конкретных методов, принципов, способов и средств построения центров управления (ЦУ) сетевой безопасности, отличительными чертами которых являются: управление инцидентами, непрерывный сетевой мониторинг, аудит конфигураций, быстрое обнаружение событий ИБ, а также автоматизированный сбор данных.

Судя по автореферату, к **новым научным** (теоретическим и инженерно-прикладным) результатам, полученным в диссертационном исследовании, следует отнести следующие:

1. Концептуальные основы и принципы построения типового ЦУ сетевой безопасности, его функциональной и организационной архитектуры, включая обеспечение собственной ИБ.

2. Таксономия, позволяющая учесть процесс определения уровня информационной защищенности ИТКС, описания функциональной деятельности организации, требующей обеспечения информационной защищенности ИТКС.

3. Описательные (неформальные) модели основных взаимосвязанных процессов управления инцидентами ИБ, требующих первоочередной реализации в ЦУ сетевой безопасности, с применением расширенного метода составления карт процессов, который позволяет оптимизировать существующие процессы путем

отслеживания избыточных действий и выявления рисков их успешной реализации.

4. Схему бизнес-логики функционирования типового ЦУ сетевой безопасности, расширенной функциональными группами модулей, отвечающими за обратную связь процессов управления сетевой безопасностью ИТКС организации, включая оперативное изменение конфигурационных настроек СЗИ в динамически изменяющейся среде функционирования ИТКС и взаимодействие с источниками информации о тенденциях в области сетевой безопасности.

5. Средство блокирования попыток компрометации массива накапливаемых в ЦУ свидетельств инцидентов ИБ в ИТКС организации.

6. Временная шкала появления технологий и средств обеспечения сетевой безопасности, что позволяет наглядно отслеживать эволюцию существующих и своевременно фиксировать появление новых технологий и средств.

Видимо, можно согласиться с автором, что указанные научные результаты вправе квалифицировать как значительное научное достижение в области обеспечения сетевой безопасности (с. 10 автореферата).

Достоверность, новизна и значимость основных научных выводов и результатов диссертационного исследования подтверждается актами о внедрении, а также отчетом о НИР № 97-07-90049 (согласно РИНЦ). В то же время глава диссертации **по оценке эффективности научных результатов** в автореферате отражена лаконично.

III. Теоретическая значимость и практическая ценность результатов исследований

Теоретическая значимость результатов состоит в создании концептуальных основ построения ЦУ сетевой безопасностью в ИТКС, а также в **развитии методов теории защиты информации** в части оригинальной систематики ИБ, архитектурных принципов и концептуальной (неформальной) модели ЦУ и пр.

Можно согласиться с автором, что **практическая ценность** исследования состоит в построении проекта типового ЦУ сетевой безопасности, а также его тематического информационного, документального и методического обеспечения. Интересным практическим приложением авторских изысканий является оригинальный глоссарий предметной области обеспечения сетевой безопасности на основе типового ЦУ, расширяющий терминологию действующего ГОСТ Р ИСО/МЭК 27033-1-2011, а также средство блокирования попыток компрометации. К достоинству работы следует отнести положительные отзывы в виде упомянутых

в автореферате актов о внедрении от компаний «ЕС-лизинг», ООО «ЛИНС-М, Qualys, а также акты о внедрении в учебный процесс от НИЯУ МИФИ и Федерального УМО.

IV. Характеристика опубликованности результатов и положений, выносимых на защиту

Опубликованность научных результатов диссертационной работы подтверждается 41-ой статьей в рецензируемых журналах, включенных в текущий перечень ВАК (согласно РИНЦ), а также 83-мя научными публикациями, проиндексированными в базе Scopus. Положения работы прошли апробацию на множестве научно-практических конференций и в учебном процессе.

Ознакомление с авторефератом и другими научными трудами автора позволяет сделать однозначный вывод, что диссертация является **единолично** написанной научно-квалификационной работой.

IV. Замечания и недостатки диссертационной работы

Несмотря на интерес к исследованию, диссертационная работа, судя по автореферату, не свободна от недостатков, в том числе методологического, понятийного и методического плана, а именно:

1. В автореферате **не приведена формальная постановка научной проблемы**, а также лаконично представлены обобщённый и частные (по каждой решаемой научной задаче) **показатели и критерии**. Это несколько затрудняет оценку завершенности работы и оценку эффективности **всех** научных результатов.

Отсутствие явных критериев бросается в глаза и далее по тексту автореферата. К примеру, на страницах 31-35 автор делает ряд вполне логичных утверждений, например, об объединении ЦИУСБ ЦИБ и СОЦ, о пяти функциональных уровнях, о невозможности рассматривать просто сочетание элементов, об «озере данных», об адекватности моделей, о выборе блокчейн для обеспечения защищенности. При этом лаконичность в указании каких-либо критериев обоснования приведенных утверждений затрудняет оценку научных результатов проведенного исследования.

В методологическом плане можно добавить, что дискуссионным является и авторское определение предмета исследования (общепринято рассматривать как область теоретических изысканий).

2. Некоторые вопросы терминологического характера, на наш взгляд, следовало бы более подробно пояснить. Например, как известно, центры

мониторинга сегмента СОПКА подразумевают контроль безопасности программного кода и атак на программный код (особенно в веб-системах, что подчеркивает автор на с.4). Однако, в предложенных классификациях «уязвимость-угроза-инцидент..» опущено понятие дефекта безопасности кода (**weakness** по аналогии с MITRE CWE и пр.). Далее на с. 27 некорректно указана атака «нулевого дня», при этом, как известно, есть только уязвимость «нулевого дня». На рис. 2 дискуссионным является разделение сетевых атак именно по указанным уровням модели OSI и др. Актуальные сегодня атаки на цепи поставок не сформулированы в явном виде.

3. При определении возможностей обеспечения ИБ ИТКС (с.5), в рамках которых она должна выполнять «упреждающее управление сетевой безопасностью», в явном виде не предусмотрен сбор и анализ данных из внешних источников. На рис. 7 также не представлены внешние источники данных об актуальных угрозах, уязвимостях, признаках компрометации, сигнатурах систем обнаружения вторжений и т.п. Отсутствие в подобной системе внешних данных указанного класса делает дискуссионным «упреждающее управление сетевой безопасностью».

На наш взгляд, автореферат бы выиграл, если бы эволюция технологий (с. 17) с учетом заявленного прогнозирования не остановилась в 2018 году.

В целом отмеченные недостатки и рекомендация принципиально не снижают научной значимости работы, так как поставленная в работе цель («разработка научно обоснованной методологии и принципов…»), судя по автореферату, достигнута. К достоинствам работы необходимо отнести прикладную направленность (в первую очередь, конкретно в плане упомянутого автором масштабного практического внедрения результатов работы), широкий кругозор, учебно-методический опыт и публикационную активность автора в тематической области, актуальность, востребованность и перспективность исследований. Автореферат характеризуется логичностью изложения, в то же время **степень формализации** представленного материала (относительно отрасли **технических** наук), на наш взгляд, является предметом обсуждения. Все выносимые положения понятны.

V. Вывод

Таким образом, судя по автореферату и печатным работам, диссертационная работа Милославской Н.Г. представляет собой законченную научно-квалификационную работу, выполненную лично соискателем на актуальную тему.

Судя по автореферату, многочисленным российским и зарубежным публикациям, а также учебно-методическим материалам и внедрениям, в диссертации разработаны научные положения, **совокупность** которых, на наш взгляд, возможно квалифицировать и как научное достижение (что аргументировано заявлено автором на с. 10 автореферата). В то же время, на наш взгляд, автором в диссертации сформулирована проблема, состоящая в разработке концептуальных основ центров управления сетевой безопасностью в информационно-телекоммуникационных сетях, имеющая важное значение для обеспечения информационной безопасности сетевых инфраструктур страны.

Полагаем, что диссертационная работа соответствует требованиям пункта 9 постановления Правительства Российской Федерации от 24.09.2013 № 842 «О порядке присуждения ученых степеней», а ее автор, Милославская Наталья Георгиевна, заслуживает присвоения ей ученой степени доктора технических наук по специальности 05.13.19 - «Методы и системы защиты информации, информационная безопасность».

Президент Акционерного общества
«Научно-производственное объединение «Эшелон»

доктор технических наук *(05.13.19 – «Методы и системы защиты информации, информационная безопасность»)*,
старший научный сотрудник

Алексей Сергеевич Марков

« 3 » февраля 2021 г.

Контактная информация:
107023; Москва, ул. Электрозаводская, 24. НПО «Эшелон»,
+7 (495) 223-2392, e-mail: a.markov@npo-echelon.ru