ПОВЫШЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИЛОВЫХ СТРУКТУР ПУТЕМ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ЦЕНТРОВ МОНИТОРИНГА БЕЗОПАСНОСТИ СЕТИ

Филин А. В.[1], Заикин Р. В.[2]

DOI:10.21681/3034-4050-2025-6-58-65

Ключевые слова: *кибератака, киберполигон, угрозы, информационная безопасность, узлы связи.*

Аннотация

Цель работы *заключается в рассмотрении зависимость информационной безопасности силовых структур от подготовки специалистов центров мониторингам безопасности сети, раскрытии предназначения центров мониторинга безопасности связи, их основных элементов, а также задач, возлагаемых на него. Также целью ставится рассмотреть способы повышения качества обучения специалистов в области информационной безопасности.*

Метод исследования: *сочетание анализа и синтеза исходных данных, моделирование обучения специалистов в условиях быстро развивающихся потенциальных угроз для информационной безопасности.*

Результаты исследования: *показаны обоснованные направления подготовки специалистов для обеспечения информационной безопасности в условиях возрастающей киберагрессии. Также выделены характерные черты оборудования киберполигонов и возможные изменения в обучении специалистов из сферы информационной безопасности.*

Практическая полезность: *теоретическая модель возможного процесса обучения, представленная в данной работе, может быть использована исследователями для написания собственных работ по теме повышения качества обучения специалистов информационной безопасности, также она может стать началом изменений к подходам в подготовке кадров.*

Введение

Начало специальной военной операции на Украине показала необходимость усиления направлений по обеспечению информационной безопасности, указанных в Доктрине информационной безопасности РФ [1], а угрозы информационной безопасности в области обороны страны явно стали реализовываться вероятным противником [2]. 20 мая 2022 года под председательством президента РФ Владимира Путина состоялось заседание Совета Безопасности РФ, на котором обсуждались вопросы повышения устойчивости и безопасности функционирования информационной инфраструктуры государства. Как отметил глава государства: «Количество кибератак на российскую информационную инфраструктуру все последние годы постоянно растёт – именно все последние годы, ну а с началом специальной военной операции на Донбассе, на Украине вызовы в этой сфере стали ещё более острыми и серьёзными, более масштабными. По сути, против России развязана настоящая агрессия, война в информационном пространстве»

Обсуждение

Анализ исследований [3] показывает, что в настоящее время в разы увеличилось число кибератак, в том числе комплексных, как отмечают специалисты, хакерам-одиночкам это, конечно же, не под силу. Атаки наносятся из разных государств, и при этом они чётко скоординированы. По сути, это действия кибервойск входящих в состав армий некоторых стран (рис. 1).

Следовательно, уже сегодня нужно самым серьёзным образом и постоянно, что называется, в режиме реального времени совершенствовать, донастраивать механизмы обеспечения информационной безопасности отраслевых критических важных объектов, от которых напрямую зависит обороноспособность нашей страны, стабильное развитие экономики и социальной сферы.

1 Филин Андрей Викторович, заместитель начальника Военно-учебного центра политехнического университета имени Петра Великого, Санкт-Петербург. Россия. E-mail: fi1y@mail.ru

2 Заикин Руслан Валерьевич, курсант факультета АСУ Военной академии связи имени Маршала Советского Союза С. М. Буденного, Санкт-Петербург. Россия. E-mail: rus.zaikin.03@mail.ru

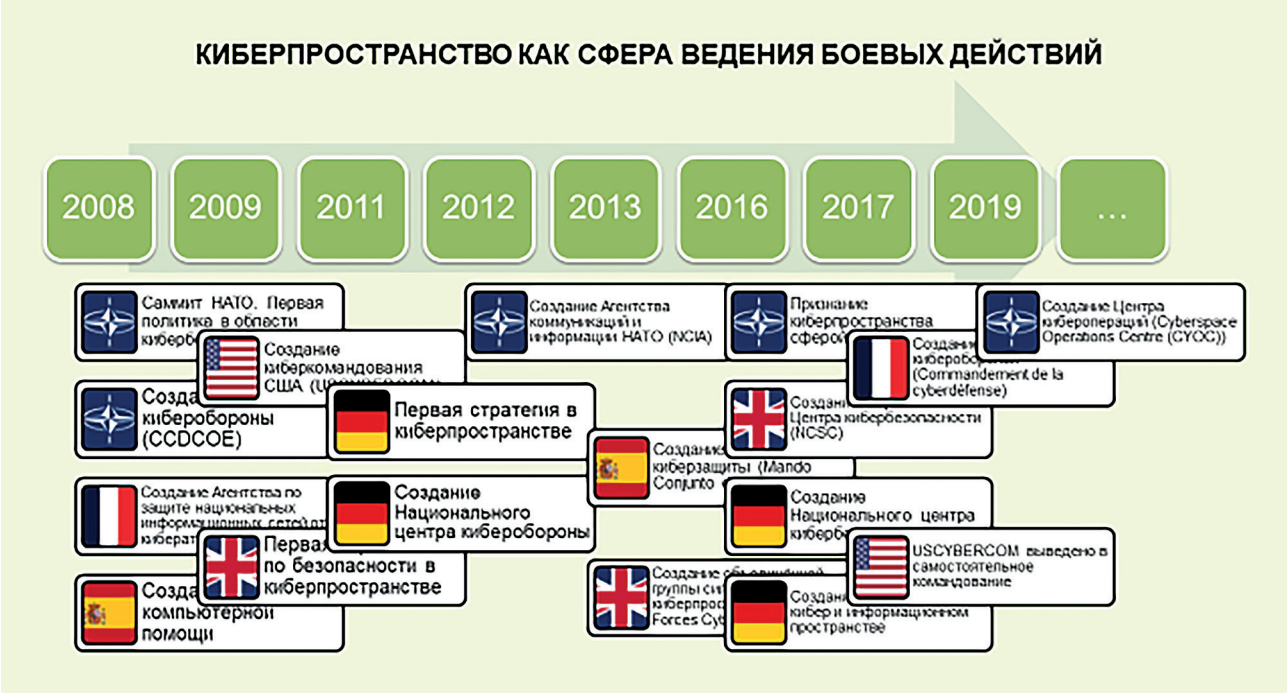

Рис. 1. Развитие киберсил в армиях стран НАТО

Согласно анализу [4] на сеть передачи данных Министерства обороны Российской Федерации (МО РФ) осуществлялась кибератака, средствами системы мониторинга трафика в сети передачи данных (СПД) МО РФ зафиксировано кратковременное пропадание связи на узле связи «Рубин-17». На графике (рис. 2.) видно пропадание трафика в период с 11.10 до 11.15.

Перед пропаданием связи зафиксирован всплеск сетевой активности по протоколу TCP по портам 3389 (RDP, служба удаленный рабочий стол) и 22 (удаленный доступ по протоколу ssh) от сетевого элемента с IP-адресом 10.129.225.1 к сетевому элементу с IP-адресу 172.20.177.83 (спутниковый маршрутизатор на КА 55 град УС «Гейзер»). С 11.05 до 11.10 между сетевыми элементами было передано 1,2 Гбайта данных (рис. 3).

Нарушение работоспособности СПД МО РФ вероятнее всего являлось следствием информационного воздействия со стороны сети связи общего пользования (ССОП). Такие инциденты информационной безопасности

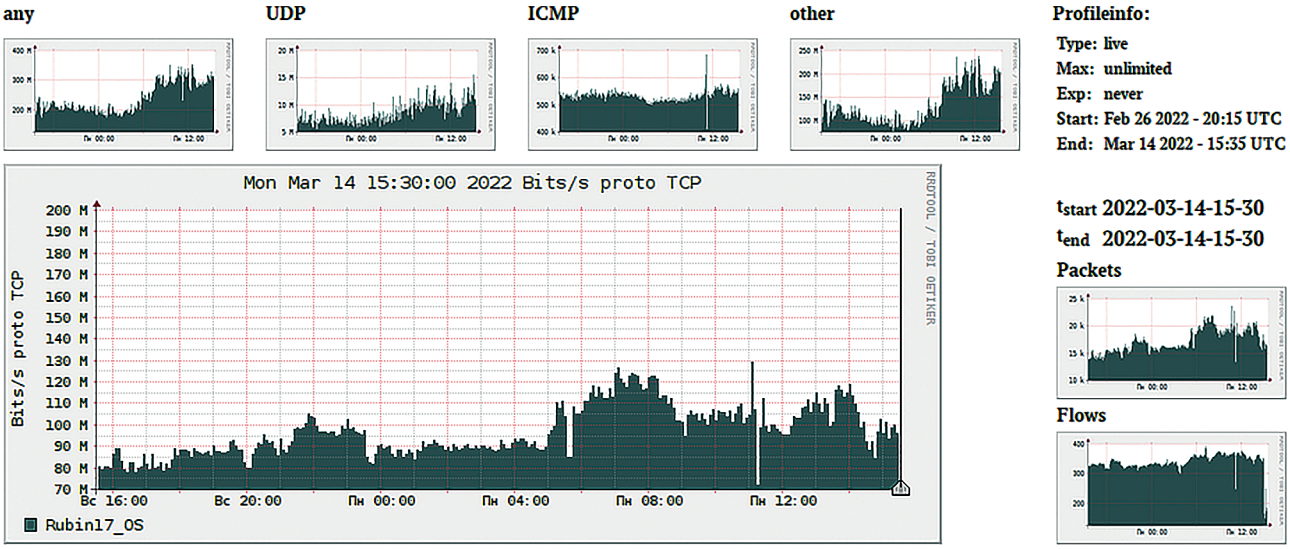

Рис. 2. Графики объективного контроля за состоянием связи на узле связи

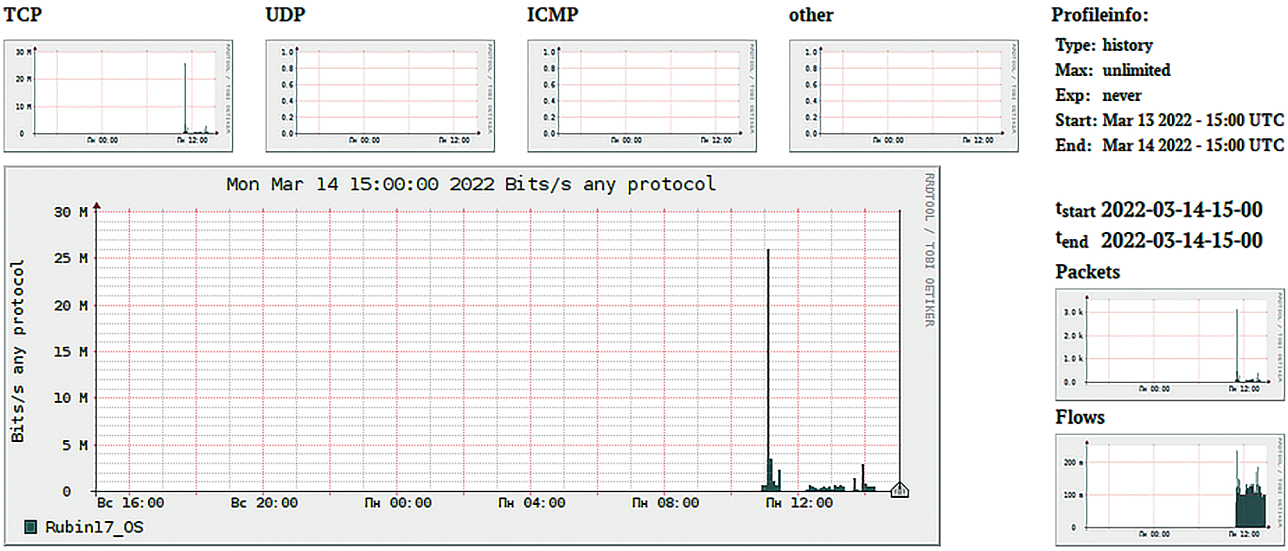

Рис. 3. Графики объективного контроля за состоянием связи на узле связи

происходят регулярно. Целью атак является не только телекоммуникационная инфраструктура МО РФ, но инфраструктура операторов ССОП, предоставляющих услуги транспортной сети (аналогичная атака была проведена 17 апреля на узлы Ростелекома, что привело к прекращению предоставления услуги на 2 часа).

Если информационно-техническое воздействие проводиться не в виде массовой атаки в целях вызвать отказ в обслуживании, то обнаружение такого воздействия является не тривиальной задачей. Оно может проявлять себя на разных сетевых элементах, и требуется сбор, и комплексная обработка данных поступающих со всех элементов системы защиты информации и сетевых устройств.

В сфере информационной безопасности эти задачи возложены на центры мониторинга информационной безопасности (Security Operations Center, SOC) [5], центр мониторинга информационной безопасности — структурное подразделение организации, отвечающее за оперативный мониторинг IT-среды и предотвращение киберинцидентов. Специалисты SOC собирают и анализируют данные с различных объектов инфраструктуры организации и при обнаружении подозрительной активности принимают меры для предотвращения атаки.

В ходе анализа кибервоздействий, подтверждается необходимость в контроле данные с различных объектов инфраструктуры и обнаружении подозрительной активности и реакции на неё. Следовательно, требуются специалисты, обладающие такими компетенциями. Чтобы раскрыть компетенцию, рассмотрим структуру и задачи, возлагаемые на Security Operations Center.

Центр мониторинга безопасности сети состоит из трёх элементов (рис. 4):

1) технические средства, обеспечивающие информационную безопасность;
2) личный состав центра мониторинга безопасности сети, выполняющий определённые роли;
3) процессы (задачи) решаемые центром безопасности сети.

Технические средства, обеспечивающие информационную безопасность, включают в себя:

- средства антивирусной защиты (САВЗ);
- средства аутентификации пользователей;
- DLP систему (предотвращает утечку данных, включает разграничение доступа к ресурсам, учёт магнитных носителей информации (МНИ), маркировку документов и т. п.);
- межсетевой экран;
- IDS/IPS (системы обнаружения и предотвращения атак);
- системы инвентаризации (сбор информации о состоянии сети);
- сканеры уязвимостей.

Сбор информации со всех этих средств осуществляет SIEM система. Также она осуществляет сбор информации из журналов событий сетевого и оконечного оборудования. Задачей

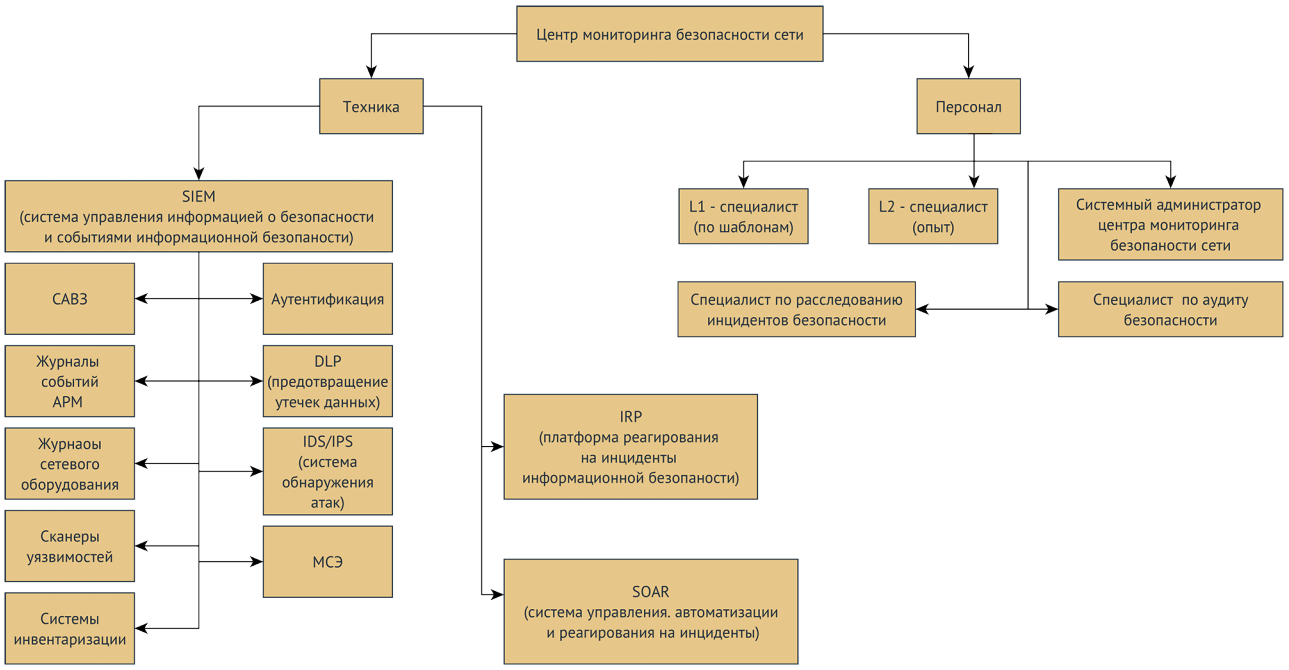

Рис. 4. Структура центра мониторинга безопасности сети

SIEM системы является не просто сбор информации, а её нормализация (т. е. приведение к общему, одинаковому виду), и поиск в этом огромном массиве данных признаков инцидентов информационной безопасности. В конечном итоге SIEM система должна сформировать событие. Обработкой этого события занимается IRP система. В принципе, это те же средства защиты информации, но автоматически выполняющие защитные действия. Например, в сети обнаруживается распространение вируса. С помощью МСЭ заражённый сегмент сети изолируется, DLP-система блокирует учётную запись пользователя и заражённый носитель, на АРМ пользователей антивирус проводит лечение. За обслуживание сценариев реагирования на различные инциденты информационной безопасности отвечает SOAR система.

Задачи, решаемые личным составом центра мониторинга безопасности сети:

1. Обработка данных в режиме реального времени.
2. Работа с внешними источниками информации (сбор, анализ новых угроз).
3. Анализ и реагирование на инциденты информационной безопасности.
4. Анализ цифровых образцов (reverse-ingeneering, программирование).
5. Обеспечение работоспособности ЦМБС:
   - обеспечение работоспособности межсетевого экрана;
   - обеспечение работоспособности системы обнаружения атак;
   - поддержание инфраструктуры ЦМБС;
   - обеспечение работоспособности сенсоров;
   - обновление сигнатур;
6. Аудит и отслеживание угроз.
7. Сбор информации и расследование внутренних угроз.
8. Сканирование сети и оценка защищённости:
   - составление карты сети;
   - сканирование на наличие уязвимостей;
   - оценка защищённости сети;
   - тестирование на проникновение.

Теоретически, эти задачи должны решаться должностными лицами службы защиты государственной тайны (ЗГТ), но на практически сетевое оборудование находится в эксплуатации у связистов, так при поступлении на снабжение войск криптомаршрутизаторов (КМ), их настройку и эксплуатацию должны были осуществлять представители службы ЗГТ, т.к. КМ относятся к средствам защиты информации, но реальна переложена на связистов. Также к ним отошли вопросы эксплуатации межсетевых экранов. В общем, служба ЗГТ оставляет за собой только контролирующую функцию, отстраняясь от практических вопросов.

Во многих воинских частях вопрос настройки системы разграничения доступа пользователей перекладывается на ответственных по защите информации.

Из всех задач, возлагаемых на SOC, курсивом задачи, которые уже выполняются офицерами связистами.

Представление о выполняемых задачах позволило сформировать функцию, которую должен будет выполнять специалист обладающей компетенцией «Способен работать на стыке двух технологий: как опытный сетевой администратор и специалист по сбору и обработке больших объёмов информации». Т.е. он должен уметь не только настроить сетевое оборудование, но и автоматизировать сбор информации с этого оборудования. Также не обходимо обрабатывать массивы данных, что сейчас отдано на откуп нейронным сетям и искусственному интеллекту. Такую компетенцию проще формировать на базе подготовки программиста. Как правило, такие обучаемые обладают инженерным мышлением и основами системного подхода. Умение разбить задачу на ряд последовательных шагов (а это и есть суть программирования – объяснить компьютеру, что делать) является базисным для инженера.

Для подготовки специалистов центра мониторинга безопасности сети предлагается примерный план подготовки. Идея, положенная в основу этого плана, заключается в следующем. Вся подготовка разбита на четыре блока, так получилось, что один блок — это календарный год. Начало обучения приходиться на второй (третий) семестр. Каркас дисциплины строится прежде всего вокруг практических занятий. Каждый блок закрывает определённую большую тему:

1) Построение комплексных узлов связи. Основы построения сети передачи данных и основы использования языка программиров ания Python.
2) Автоматизация администрирования (на основе скриптов Python). Основы информационной безопасности.
3) Построение системы защиты информации. Автоматизация сбора данных с различных устройств в SIEM.
4) Администрирование SOC. Обработка больших данных (Data mining, нейросети и искусственный интеллект). Расследование инцидентов информационной безопасности.

Каждый блок (учебный год) разбит на два этапа. В первом (2 зачётные единицы) этапе даётся необходимый объём теоретических знаний и проводятся практические занятия. Заканчивается этап зачётом с оценкой. На втором этапе (1 з.е.) обучающиеся разрабатывают свой проект из предметной области первого этапа. Они должны будут решить определённую прикладную задачу. Проходит второй этап в форме курсового проекта, которому предшествует семинар. На семинаре определяются направления и рамки проектов. Заканчивается этап защитой курсового проекта [6].

Особое внимание должно быть уделено организации самоподготовке. Самостоятельная работа обучающихся – ключевой фактор успеха в формировании заявленной компетенции. Объём передаваемых знаний для данной дисциплины огромен и обширен, и не представляется возможным его передача только репродуктивным и объяснительно-иллюстративным методами обучения.

В качестве отправной точки в формирования учебно-материальной базы должен служить – киберполигон. Киберполигон – это комплекс виртуальных инфраструктур и технических средств, повторяющих типовые инфраструктуры системы связи (полунатурное моделирование) на основе применения эмулятора сетевых технологий EVE-NG, функционирующих на сертифицированных программных средствах операционной системы «ASTRA LINUX», программного средства виртуализации [7].

При создании киберполигона необходимо использовать типовую схему сетевой инфраструктуры системы военной связи – это достаточно стандартный набор серверов, рабочих компьютеров и различных сетевых устройств с типовым набором программного обеспечения элементов сети и системы военной связи с элементами предоставления различного рода услуг, а также систем информационной безопасности этой сети и системы в целом [8].

Все оборудование киберполигона взаимодействует между собой так же, как и в реальной киберфизической системе. В рамках такого подхода киберфизическая сеть и система военной связи частично моделируется с помощью реального оборудования и с помощью виртуальных образов реального оборудования, развернутых в виртуальной среде [9].

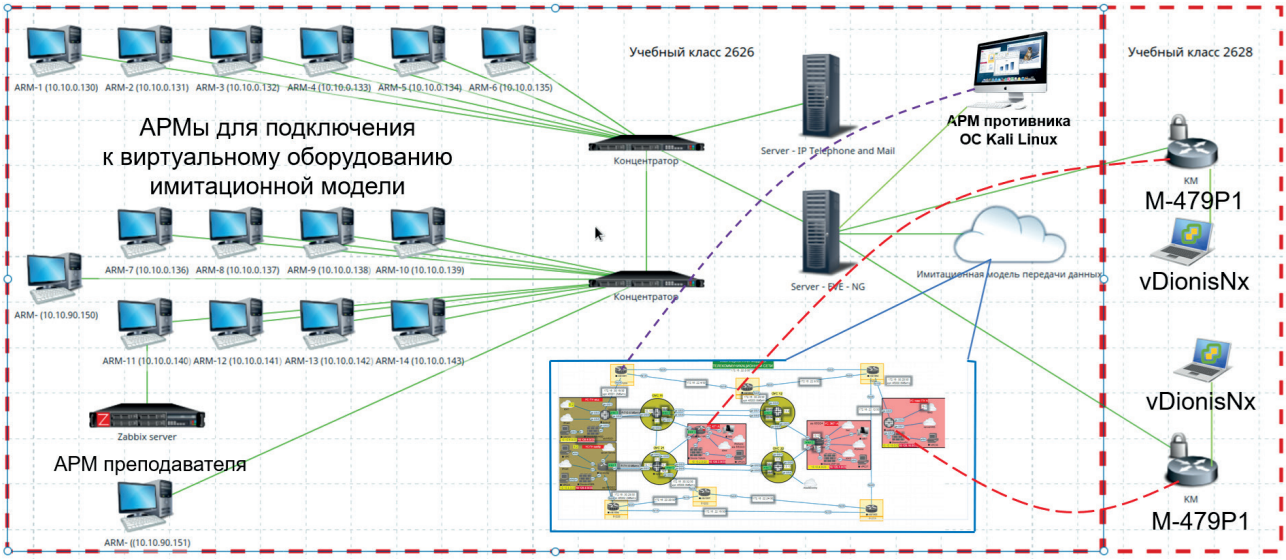

Рис. 5. Вариант оборудования киберполигона

Если говорить более предметно, то при построении этой модели предлагается использовать следующее оборудование и вычислительные средства:

- автоматизированное рабочее место оператора с установленным программным обеспечением операционной системы «Astra Linux», средств виртуализации для систем:
- мониторинга;
- анализа трафика компьютерных сетей Ethernet и других возможных программ;
- сбора информации о трафике, проходящем через телекоммуникационное оборудование;
- образы телекоммуникационного оборудования инфокоммуникационной сети системы военной связи использовался:
- граничный маршрутизатор узла с функциями межсетевого экрана;
- граничный маршрутизатор узла из состава аппаратная П-243П, МК ЗВКС, стационарные узлы связи МО РФ;
- маршрутизирующий коммутатор;
- граничный маршрутизатор [10].

Заключение

Исходя их выше представленного, задача подготовки специалистов по кибербезопасности в ВС РФ является актуальной. Для её решения, в первую очередь, необходимо выработать общий подход к киберсфере и дать его чёткое определение. На основе опыта подготовки специалистов по кибербезопасности, целесообразно их готовить из программистов и инженеров в области телекоммуникаций. Подготовка имеет яркую практическую направленность. Можно говорить о том, что не имея технологической компетенции (знания о том, как работает телекоммуникационная сеть) невозможно защитить киберсферу. Наличие развитой компетенции диктует необходимость отбора для дальнейшего обучения наиболее отличившихся в учебе.

Точное наполнение и рамки области знаний – эти вопросы остаются открытыми для дискуссии. В любом случае, две предпосылки для подготовки специалистов по кибербезопасности останутся без изменений: практическая направленность подготовки и необходимость знаний о сетях и системах передачи данных.

Литература

1. Курилкин А. В. Информационные и кибернетические операции как инструмент реализации внешней политики: формы, методы, технологии. Диссертация кандидата политических наук. М. С. 285.
2. Иванов В. Г. Основы построения и оценки эффективности функционирования системы связи специального назначения в международном вооруженном конфликте на основе многосферной и конвергентной структуры ее элементов: Монография. – СПб.: ПОЛИТЕХ, 2023. – 298 с.

3. Свинарев С. В. Пути повышения эффективности обеспечения информационной безопасности / С. В. Свинарев, В. Н. Галкин, Т. В. Медведева // Право и управление. – 2024. – № 3. – С. 15–18. – DOI: 10.24412/2224-9133-2024-3-15-18. – EDN YRPNMG.
4. Гавриленко А. И. Методы повышения эффективности информационной безопасности / А. И. Гавриленко, А. В. Лубенцов // Техника и безопасность объектов уголовно-исполнительной системы: сборник материалов Международной научно-практической конференции, Воронеж, 22–23 мая 2024 года. – Воронеж: Строки, 2024. – С. 19–21. – EDN UXIRAW.
5. Давидюк С. А. Мониторинг функционирования операционной системы специального назначения / С. А. Давидюк // Информационные технологии и информационная безопасность в профессиональной деятельности: Сборник научных статей II Межвузовской научно-практической конференции с международным участием, Новосибирск, 01 февраля 2023 года. – Новосибирск: Новосибирский военный институт имени генерала армии И. К. Яковлева войск национальной гвардии Российской Федерации, 2023. – С. 51–54. – EDN CYIERP.
6. Семенов С. В. Повышение информационной безопасности в цифровой среде образовательной организации / С. В. Семенов, В. М. Кудрявцев // XII Лужские научные чтения. Современное научное знание: теория и практика: Материалы международной научной конференции, Санкт-Петербург, 22 мая 2024 года. – Санкт-Петербург: Ленинградский государственный университет им. А. С. Пушкина, 2024. – С. 24–27. – EDN GONWGJ.
7. Хорзова И. С. Концепция создания киберполигона для обучения специалистов в области информационной безопасности / И. С. Хорзова // Информационные технологии в деятельности органов внутренних дел: Сборник научных статей, Москва, 22 апреля 2021 года. – Москва: Московский университет Министерства внутренних дел Российской Федерации им. В. Я. Кикотя, 2021. – С. 172–176. – EDN ZBMZDX.
8. Афанасьева М. В. Разработка модуля киберполигона, полноценно имитирующего компьютерные атаки / М. В. Афанасьева, Д. Р. Абзалутдинов, К. Я. Бараков // Актуальные проблемы современной науки, техники и образования : Тезисы докладов 81-й международной научно-технической конференции, Магнитогорск, 17–21 апреля 2023 года. Том 1. – Магнитогорск: Магнитогорский государственный технический университет им. Г. И. Носова, 2023. – С. 406. – EDN TWBKGJ.
9. Рытов М. Ю. Организация киберполигона как основополагающая часть формирования компетенций обучающегося по направлению «информационная безопасность» / М. Ю. Рытов, М. М. Голембиовский // Информационные технологии в управлении и моделировании мехатронных систем: Материалы II научно-практической международной конференции, Тамбов, 14–16 октября 2020 г. – Тамбов: Тамбовский государственный технический университет, 2020. – С. 80-83. – EDN OLHNTV.
10. Баранов В. В. Разработка и внедрение киберполигона в процесс подготовки специалистов по защите информации / В. В. Баранов, А. П. Корчагина // Вестник Военного инновационного технополиса «Эра». – 2022. – Т. 3, № 4. – С. 401–406. – DOI 10.56304/S2782375X22040027. – EDN OMWITG.

IMPROVING THE INFORMATION SECURITY OF LAW ENFORCEMENT AGENCIES THROUGH THE TRAINING OF SPECIALISTS FROM NETWORK SECURITY MONITORING CENTERS

Filin A. V.[3], Zaikin R. V.[4]

Keywords: *cyberattack, cyber range, threats, information security, communication nodes.*

Abstract

The purpose of the work *is to consider the dependence of information security of law enforcement agencies on the training of specialists in network security monitoring centers, to reveal the purpose of communication security monitoring centers, their main elements, as well as the tasks assigned to it. The goal is also to consider ways to improve the quality of training of specialists in the field of information security.*

3 Andrey V. Filin, Deputy Head of the Military Training Center of Peter the Great Polytechnic University, St. Petersburg. Russia. E-mail: fi1y@mail.ru

4 Ruslan V. Zaikin, cadet of the Faculty of Automated Control Systems of the Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny, St. Petersburg. Russia. E-mail: rus.zaikin.03@mail.ru

Метод исследования: сочетание анализа и синтеза исходных данных, моделирование обучения специалистов в условиях быстро развивающихся потенциальных угроз для информационной безопасности.

Результаты исследования: показаны обоснованные направления подготовки специалистов для обеспечения информационной безопасности в условиях возрастающей киберагрессии. Также выделены характерные черты оборудования киберполигонов и возможные изменения в обучении специалистов из сферы информационной безопасности.

Практическая полезность: теоретическая модель возможного процесса обучения, представленная в данной работе, может быть использована исследователями для написания собственных работ по теме повышения качества обучения специалистов информационной безопасности, также она может стать началом изменений к подходам в подготовке кадров.

References

1. Kurilkin A. V. Informacionnye i kiberneticheskie operacii kak instrument realizacii vneshnej politiki: formy, metody, tehnologii. Dissertacija kandidata politicheskih nauk. M. S. 285.
2. Ivanov V. G. Osnovy postroenija i ocenki jeffektivnosti funkcionirovanija sistemy svjazi special'nogo naznachenija v mezhdunarodnom vooruzhennom konflikte na osnove mnogosfernoj i konvergentnoj struktury ee jelementov: Monografija. – SPb.: POLITEH, 2023. – 298 s.
3. Svinarev, S. V. Puti povyshenija jeffektivnosti obespechenija informacionnoj bezopasnosti / S. V. Svinarev, V. N. Galkin, T. V. Medvedeva // Pravo i upravlenie. – 2024. – № 3. – S. 15–18. – DOI: 10.24412/2224-9133-2024-3-15-18. – EDN YRPNMG.
4. Gavrilenko, A. I. Metody povyshenija jeffektivnosti informacionnoj bezopasnosti / A. I. Gavrilenko, A. V. Lubencov // Tehnika i bezopasnost' ob#ektov ugolovno-ispolnitel'noj sistemy: sbornik materialov Mezhdunarodnoj nauchno-prakticheskoj konferencii, Voronezh, 22–23 maja 2024 goda. – Voronezh: Stroki, 2024. – S. 19–21. – EDN UXIRAW.
5. Davidjuk, S. A. Monitoring funkcionirovanija operacionnoj sistemy special'nogo naznachenija / S. A. Davidjuk // Informacionnye tehnologii i informacionnaja bezopasnost' v professional'noj dejatel'nosti: Sbornik nauchnyh statej II Mezhvuzovskoj nauchno-prakticheskoj konferencii s mezhdunarodnym uchastiem, Novosibirsk, 01 fevralja 2023 goda. – Novosibirsk: Novosibirskij voennyj institut imeni generala armii I. K. Jakovleva vojsk nacional'noj gvardii Rossijskoj Federacii, 2023. – S. 51–54. – EDN CYIERP.
6. Semenov, S. V. Povyshenie informacionnoj bezopasnosti v cifrovoj srede obrazovatel'noj organizacii / S. V. Semenov, V. M. Kudrjavcev // XII Luzhskie nauchnye chtenija. Sovremennoe nauchnoe znanie: teorija i praktika : Materialy mezhdunarodnoj nauchnoj konferencii, Sankt-Peterburg, 22 maja 2024 goda. – Sankt-Peterburg: Leningradskij gosudarstvennyj universitet im. A.S. Pushkina, 2024. – S. 24–27. – EDN GONWGJ.
7. Horzova, I. S. Koncepcija sozdanija kiberpoligona dlja obuchenija specialistov v oblasti informacionnoj bezopasnosti / I. S. Horzova // Informacionnye tehnologii v dejatel'nosti organov vnutrennih del: Sbornik nauchnyh statej, Moskva, 22 aprelja 2021 goda. – Moskva: Moskovskij universitet Ministerstva vnutrennih del Rossijskoj Federacii im. V. Ja. Kikotja, 2021. – S. 172–176. – EDN ZBMZDX.
8. Afanas'eva, M. V. Razrabotka modulja kiberpoligona, polnocenno imitirujushhego komp'juternye ataki / M. V. Afanas'eva, D. R. Abzalutdinov, K. Ja. Barakov // Aktual'nye problemy sovremennoj nauki, tehniki i obrazovanija : Tezisy dokladov 81-j mezhdunarodnoj nauchno-tehnicheskoj konferencii, Magnitogorsk, 17–21 aprelja 2023 goda. Tom 1. – Magnitogorsk: Magnitogorskij gosudarstvennyj tehnicheskij universitet im. G. I. Nosova, 2023. – S. 406. – EDN TWBKGJ.
9. Rytov, M. Ju. Organizacija kiberpoligona kak osnovopolagajushhaja chast' formirovanija kompetencij obuchajushhegosja po napravleniju «informacionnaja bezopasnost'» / M. Ju. Rytov, M. M. Golembiovskij // Informacionnye tehnologii v upravlenii i modelirovanii mehatronnyh sistem: Materialy II nauchno-prakticheskoj mezhdunarodnoj konferencii, Tambov, 14–16 oktjabrja 2020 goda. – Tambov: Tambovskij gosudarstvennyj tehnicheskij universitet, 2020. – S. 80–83. – EDN OLHNTV.
10. Baranov, V. V. Razrabotka i vnedrenie kiberpoligona v process podgotovki specialistov po zashhite informacii / V. V. Baranov, A. P. Korchagina // Vestnik Voennogo innovacionnogo tehnopolisa «Jera». – 2022. – T. 3, № 4. – S. 401–406. – DOI 10.56304/S2782375X22040027. – EDN OMWITG.