

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»

**РУКОВОДСТВО АДМИНИСТРАТОРА ПРОГРАММНО-
АППАРАТНОГО КОМПЛЕКСА CHECKPOINT**

Выпускная квалификационная работа
по направлению подготовки 44.03.04 Профессиональное обучение
(по отраслям)
профилю подготовки «Информатика и вычислительная техника»
специализации «Информационная безопасность»

Идентификационный номер ВКР: 607

Екатеринбург 2019

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»
Институт инженерно-педагогического образования
Кафедра информационных систем и технологий

К ЗАЩИТЕ ДОПУСКАЮ

Заведующий кафедрой ИС

_____ И. А. Сулова

« ____ » _____ 2019 г.

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
РУКОВОДСТВО АДМИНИСТРАТОРА ПРОГРАММНО-
АППАРАТНОГО КОМПЛЕКСА СНЕСКРОИПТ**

Исполнитель:

обучающийся группы ЗИБ-401С

А. В. Китанин

Руководитель:

канд. пед. наук, доцент

К. А. Федулова

Нормоконтролер:

Н. В. Хохлова

Екатеринбург 2019

АННОТАЦИЯ

Выпускная квалификационная работа состоит из руководства администратора программно-аппаратного комплекса Checkpoint и пояснительной записки на 58 страницах, содержащей 35 рисунков, 30 источников литературы и одно приложение на двух страницах.

КЛЮЧЕВЫЕ СЛОВА: СНЕСКРОИПТ, РУКОВОДСТВО АДМИНИСТРАТОРА, ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, НПЦ «ПРОМЭЛЕКТРОНИКА»

Китанин А. В., Руководство администратора программно-аппаратного комплекса Checkpoint: выпускная квалификационная работа / А. В. Китанин; Рос. гос. проф.-пед. ун-т, Ин-т инж.-пед. образования, Каф. информ. систем и технологий. — Екатеринбург, 2019. — 58 с.

В работе рассмотрены вопросы, связанные с выбором программного обеспечения для разработки руководства, а также процесс разработки.

Целью, выпускной квалификационной работы, является разработка руководства администратора программно-аппаратного комплекса Checkpoint.

Для достижения цели были поставлены задачи: определить понятие руководства администратора и требования к его реализации, проанализировать требования, предъявляемые к интерфейсу руководства администратора, выбрать программные средства для реализации руководства пользователя, реализовать руководство администратора для информационной системы.

Руководство администратора позволяет организовать процесс обучения сотрудников компании работе с программно-аппаратным комплексом Checkpoint и решению задач по его настройке.

СОДЕРЖАНИЕ

Введение.....	4
1 Анализ программно-аппаратного комплекса Checkpoint	6
1.1 Устройство информационной безопасности.....	6
1.2 Основные типы устройств информационной безопасности.....	7
1.3 Описание компонентов программно-аппаратного комплекса Checkpoint	10
1.4 Программные блейды (Checkpoint Software Blades)	11
1.5 Определение руководства администратора и требования к его реализации	24
1.6 Выбор программных средств для реализации руководства администратора	29
2 Разработка электронного руководства администратора программно-аппаратного комплекса Checkpoint	35
2.1 Цель и назначение руководства администратора программно-аппаратного комплекса.....	35
2.2 Общее описание структуры и интерфейса руководства администратора	36
2.3 Содержание руководства администратора.....	45
2.4 Методические рекомендации по использованию руководства.....	49
2.5 Апробация руководства администратора.....	50
Заключение	51
Список использованных источников	53
Приложение	57

ВВЕДЕНИЕ

Информация, поддерживающие ее процессы, информационные системы и сетевая инфраструктура являются существенными активами организации. Конфиденциальность, целостность и доступность информации могут существенно способствовать обеспечению конкурентоспособности, ликвидности, доходности, соответствия законодательству и деловой репутации организации.

Организации, их информационные системы и сети все чаще сталкиваются с различными угрозами безопасности, такими как компьютерное мошенничество, шпионаж, вредительство, вандализм, пожары или наводнения. Такие источники ущерба, как компьютерные вирусы, компьютерный взлом и атаки типа отказа в обслуживании, становятся более распространенными, более агрессивными и все более изощренными.

На предприятии акционерное общество (АО) «Научно-производственный центр (НПЦ) “Промэлектроника”», основным видом деятельности которого является разработка систем безопасности движения поездов на магистральных железных дорогах, подъездных путях промышленных предприятий и в метрополитене, было решено выделить средства бюджета на приобретение и внедрение программно-аппаратного комплекса (ПАК) Checkpoint [18], для усиления защиты информации.

После внедрения программно-аппаратного комплекса Checkpoint на предприятии было решено написать документ «Руководство администратора», который относится к пакету эксплуатационной документации. Основная цель документа «Руководство администратора» заключается в обеспечении администратора комплекса необходимой информацией для самостоятельной работы с программой или автоматизированной системой. Документ должен отвечать на следующие вопросы: назначение комплекса, его возможности; что необходимо для обеспечения его корректного функционирования и, что

делать в случае отказа системы. Разработка самого программного продукта выполнена в виде инструкций для выполнения основных функций необходимых для администрирования.

Объектом выпускной квалификационной работы является процесс обучения сотрудников основным принципам работы с ПАК Checkpoint, а также устранение возможных неисправностей, которые могут возникнуть в процессе эксплуатации комплекса.

Предметом выпускной квалификационной работы является сопроводительная документация, прилагаемая к оборудованию программно-аппаратного комплекса, а также информация по эксплуатации, настройке и устранению неисправностей с официального сайта Checkpoint, представленная только на иностранном языке.

Цель выпускной квалификационной работы — разработать руководство администратора программно-аппаратного комплекса Checkpoint.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Определить понятие руководства администратора и требования к его реализации.
2. Проанализировать требования, предъявляемые к интерфейсу руководства администратора программно-аппаратным комплексом Checkpoint.
3. Выбрать программные средства для реализации руководства пользователя.
4. На основе анализа требований и выбранных средств разработать структуру и интерфейс руководства администратора для информационной системы программно-аппаратным комплексом Checkpoint.
5. Реализовать руководство администратора для информационной системы программно-аппаратного комплекса Checkpoint.

1 АНАЛИЗ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА CHECKPOINT

1.1 Устройство информационной безопасности

Зависимость от информационных систем и услуг означает, что организации становятся все более уязвимыми по отношению к угрозам безопасности. Взаимодействие сетей общего пользования и частных сетей, а также совместное использование информационных ресурсов затрудняет управление доступом к информации. Тенденция к использованию распределенной обработки данных ослабляет эффективность централизованного контроля. При проектировании многих информационных систем вопросы безопасности не учитывались. Уровень безопасности, который может быть достигнут техническими средствами, имеет ряд ограничений и, следовательно, должен сопровождаться надлежащими организационными мерами. Выбор необходимых мероприятий по управлению информационной безопасностью требует тщательного планирования и внимания к деталям.

Управление информационной безопасностью нуждается, как минимум, в участии всех сотрудников организации. Также может потребоваться участие поставщиков, клиентов или акционеров. Кроме того, могут потребоваться консультации специалистов сторонних организаций. Мероприятия по управлению в области информационной безопасности обойдутся значительно дешевле и окажутся более эффективными, если будут включены в спецификацию требований на стадии проектирования системы.

Устройством информационной безопасности обычно называют специализированный сервер, предназначенный для защиты сети от нежелательного трафика — последний блокируется средствами встроенного межсетевого экрана, посредством фильтрации контента или с помощью антивируса, при этом система обнаружения вторжений (Intrusion detection system — IPS) мо-

жет выводить отчет о попытке «взлома» или инициировать предписанные правилами защитные меры. Для защиты трафика используются технологии Secure Socket Layer Virtual Private Network/ IP Security Virtual Private Network (SSL VPN/IPSec VPN) и шифрование.

Такие устройства служат в качестве шлюзов безопасности, однако некоторые могут использоваться и для оценки уязвимости сети, а также предотвращения утечек данных (Data Loss Prevention — DLP) и контроля доступа пользователей к ресурсам корпоративной сети и Интернета. В унифицированных устройствах (Unified Threat Management — UTM) объединяются несколько средств безопасности (межсетевой экран, VPN, антивирус и др.). UTM — самый крупный сегмент рынка устройств безопасности, указано на рисунке 1.

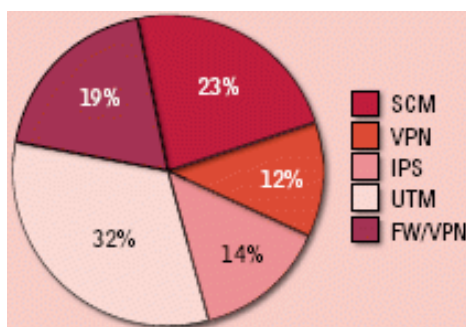


Рисунок 1 — Сегменты рынка

По мнению экспертов компании Leta IT, системы комплексной безопасности — прогнозируемая эволюция разрозненных решений информационной безопасности (ИБ). В то же время эксперты IBM говорят о том что, унификация средств обеспечения ИБ на одной платформе помогает организациям эффективнее управлять сетевой безопасностью, клиентскими приложениями, безопасностью данных и приложений Web.

1.2 Основные типы устройств информационной безопасности

UTM должны быть просты в настройке и использовании, предусматривать централизованное управление. Ввиду ограниченной производительности

и функциональности UTM больше всего подходят для использования в малых/средних компаниях или филиалах распределенного предприятия. Как сообщают специалисты компании Juniper, решения UTM позволяют значительно сократить расходы и в то же время обеспечить защиту филиала, при этом в одном устройстве сочетаются сервисы маршрутизации, функции коммутации и межсетевое экранирование. В России рынок UTM только начинает набирать обороты. По данным Leta IT, хотя всплеск интереса к UTM наметился еще в 2008 году, он не привел к существенному росту продаж этого оборудования, несмотря на увеличение доли подобных продуктов. Однако с возобновлением роста российского рынка информационных технологий (ИТ) в целом и рынка ИБ в частности ситуация меняется.

Unified Threat Management (UTM) — консолидация нескольких средств защиты в одном решении. Самый распространенный вариант это: межсетевой экран, IPS, Proxy (Uniform Resource Locator (URL) фильтрация), потоковый Antivirus, Anti-Spam, VPN и так далее. Все это объединяется в рамках одного UTM решения, что проще с точки зрения интеграции, настройки, администрирования и мониторинга, а это в свою очередь положительно сказывается на общей защищенности сети. Когда UTM решения только появились, то их рассматривали исключительно для небольших компаний, т.к. UTM не справлялись с большими объемами трафика. Связано это было с двумя основными причинами:

1. Способ обработки пакетов. Первые версии UTM решений обрабатывали пакеты последовательно, каждым «модулем». Пример: сначала пакет обрабатывается межсетевым экраном, затем IPS, потом его проверяет антивирус и так далее. Естественно, что такой механизм вносил серьезные задержки в трафик и сильно расходовал ресурсы системы (процессор, память).

2. Слабое «железо». Как было сказано выше, последовательная обработка пакетов сильно отъедала ресурсы и «железо» тех времен (1995–2005) просто не справлялось с большим трафиком.

Но прогресс не стоит на месте. С тех пор значительно увеличились аппаратные мощности, а обработка пакетов изменилась (надо признать, что далеко не у всех вендоров) и стала позволять практически одновременный анализ сразу в нескольких модулях (Межсетевой экран, IPS, AntiVirus и т.д.). Современные UTM решения могут «переваривать» десятки и даже сотни гигабит в режиме глубокого анализа, что дает возможность использовать их в сегменте крупного бизнеса или даже дата центров.

На рисунке 2 представлен знаменитый магический квадрант Гартнера для UTM решений за август 2016 года.



Рисунок 2 — Квадрант Гартнера

NGFW — Next Generation Firewall

Название говорит само за себя — межсетевой экран следующего поколения. Данный концепт появился значительно позже, чем UTM. Главная идея NGFW — глубокий анализ пакетов (DPI) с помощью встроенного IPS и разграничение доступа на уровне приложений (Application Control). В данном случае IPS как раз и нужен, чтобы в потоке пакетов выявлять то или иное приложение, что позволяет разрешить, либо запретить его. Пример: мы можем разрешить работу Skype, но запретить передачу файлов. Можем запре-

тить использовать Torrent или Remote Desktop Protocol (RDP). Также поддерживаются Web-приложения: Можно разрешить доступ к VK.com, но запретить игры, сообщения или просмотр видео. По сути, качество NGFW зависит от количества приложений, которые он может определять.

1.3 Описание компонентов программно-аппаратного комплекса Checkpoint

Checkpoint имеет три основных составляющих, как изображено на рисунке 3 [19]:

1. **Security Gateway (SG)** — собственно сам шлюз безопасности, который как правило ставится на периметр сети и выполняет функции межсетевого экрана, потокового антивируса, антибота, IPS и т.д.

2. **Security Management Server (SMS)** — сервер управления шлюзами. Практически все настройки на шлюзе (SG) выполняются с помощью данного сервера. Security Management Server (SMS) также может выступать в качестве лог-сервера и обрабатывать их встроенной системой анализа и корреляции событий — Smart Event (подобие SIEM для Checkpoint). SMS используется для централизованного управления несколькими шлюзами (количество шлюзов зависит от модели SMS, либо от лицензии), однако использование обязательно, даже если имеется всего один шлюз. Тут следует отметить, что Checkpoint одни из первых стали применять подобную централизованную систему управления, которая уже много лет подряд признается «золотым стандартом» по отчетам компании Gartner.

3. **Smart Console** — клиентская консоль для подключения к серверу управления (SMS). Как правило, устанавливается на компьютер администратора. Через эту консоль осуществляются все изменения на сервере управления, а уже после этого можно применить настройки к шлюзам безопасности (Install Policy).

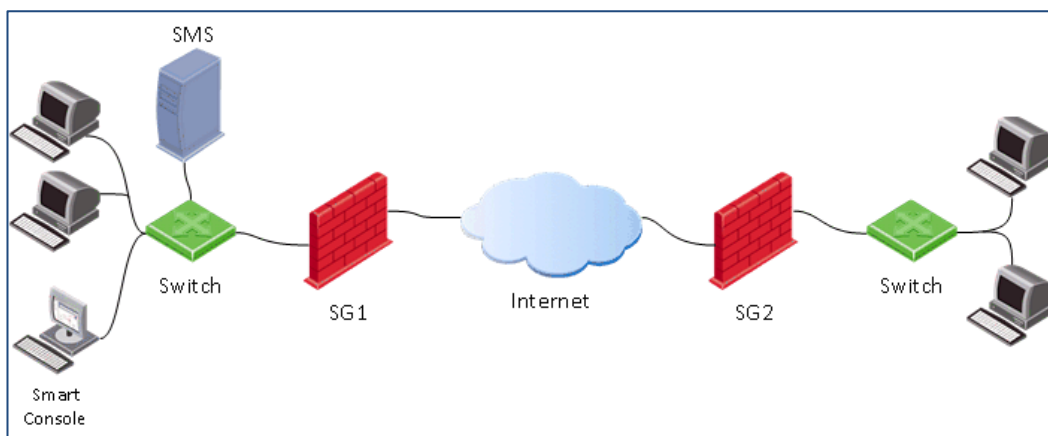


Рисунок 3 — Типичная схема установки Checkpoint

В целом смарт консоль состоит из нескольких отдельных программ, они показаны на рисунке 4.

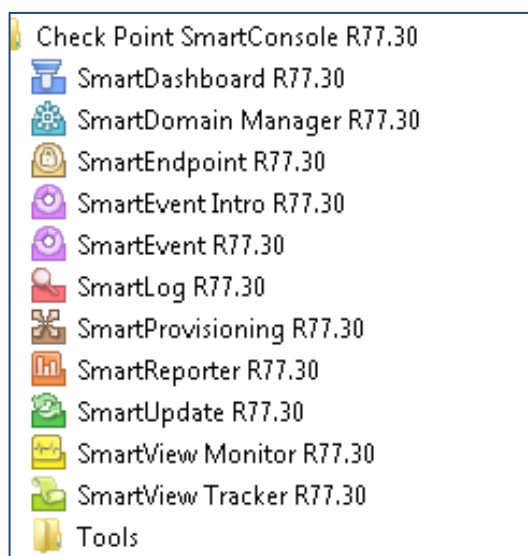


Рисунок 4 — Программы входящие в состав SmartConsole

Каждая отвечает за свой функционал, такой как администрирование, анализ данных, обновление программного обеспечения (ПО), наблюдение за состоянием оборудования.

1.4 Программные блейды (Checkpoint Software Blades)

Для **Security Center** (функционал шлюза):

- Firewall — функционал межсетевого экрана;
- IPSec VPN — построение частные виртуальных сетей;

- Mobile Access — удаленный доступ с мобильных устройств;
- IPS — система предотвращения вторжений;
- Anti-Bot — защита от ботнет сетей;
- AntiVirus — потоковый антивирус;
- AntiSpam & Email Security — защита корпоративной почты;
- Identity Awareness — интеграция со службой Active Directory;
- Monitoring — мониторинг практически всех параметров шлюза (load, bandwidth, VPN статус и т.д.);
 - Application Control — межсетевой экран уровня приложений (функционал NGFW);
 - URL Filtering — безопасность Web (+функционал проху);
 - Data Loss Prevention — защита от утечек информации (DLP);
 - Threat Emulation — технология песочниц (SandBox);
 - Threat Extraction — технология очистки файлов;
 - QoS — приоритезация трафика.

Для Management (функционал сервера управления):

- Network Policy Management — централизованное управление политиками;
- Endpoint Policy Management — централизованное управление агентами Checkpoint (Checkpoint производит решения не только для сетевой защиты, но и для защиты рабочих станций (ПК) и смартфонов);
 - Logging & Status — централизованный сбор и обработка логов;
 - Management Portal — управление безопасностью из браузера;
 - Workflow — контроль над изменением политик, аудит изменений и т.д.;
- User Directory — интеграция с Lightweight Directory Access Protocol (LDAP);
 - Provisioning — автоматизация управления шлюзами;
 - Smart Reporter — система отчетности;

- Smart Event — анализ и корреляция событий (SIEM);
- Compliance — автоматическая проверка настроек и выдача рекомендаций.

Так как программных блейдов более 20 штук, подробнее рассмотрим лишь некоторые из них.

Программный блейд «URL Filtering» — программное обеспечение Checkpoint использует облачную классификацию URL, возможность проверки SSL и интеграцию с блейдом Application Control реализуя единое управление всеми аспектами Web-безопасности.

Функции:

- динамическая облачная классификация;
- разрешает, блокирует или ограничивает доступ к более чем 100 миллионов сайтов и анализирует зашифрованный SSL-трафик;
- вовлекает и обучает пользователей с помощью UserCheck посредством мгновенных предупреждений Web-политики;

Программный блейд Checkpoint URL Filtering защищает компании и пользователей, путем использования облачной классификации свыше 100 миллионов Web-сайтов. URL Filtering обеспечивает полностью интегрированную в шлюз оптимизированную Web-безопасность, предотвращая возможность обхода через внешние прокси-серверы; интеграцию принудительного использования политик с Application Control для абсолютной защищенности Web и Web 2.0 и использование UserCheck для расширения возможностей и обучения пользователей политике использования Интернет в режиме реального времени. Кроме того, может быть отсканирован и защищен зашифрованный SSL-трафик внутри шлюза.

URL Filtering использует динамически обновляемую базу данных из более чем 100 миллионов Web-сайтов для разрешения, блокирования или ограничения доступа к Web-сайтам в режиме реального времени — всего трафика, явного и зашифрованного SSL. Предлагается выбор из более чем 50 predetermined разделов по информационному наполнению. Объединение

Программных блейдов URL Filtering и Application Control унифицирует контроль доступа к Web-сайту с Интернет приложением и контроль за виджетами для повышения безопасности [15].

Программный блейд Checkpoint URL Filtering дает возможность разрешать, блокировать или ограничивать доступ к миллионам Web-сайтов и Web-страниц. Программный блейд Checkpoint Application Control предоставляет аналогичные возможности для 4,500 Интернет приложений и более 225,000 Web-виджетов, в случае срабатывания блейда, пользователь, зашедший на ненадежный сайт, получит уведомление, на примере скриншота изображенного на рисунке 5.



Рисунок 5 — ЮзерЧек

Сканируется и защищается зашифрованный SSL-трафик проходящий через шлюз. Когда трафик проходит через шлюз, шлюз расшифровывает его с помощью открытого ключа отправителя, проверяет и защищает, затем повторно шифрует, отправляя вновь зашифрованное содержимое получателю.

Детализировано определяются исключения для проверки SSL, чтобы защитить конфиденциальность пользователей и выполнить требования корпоративной политики. Некоторый зашифрованный контент, проходящий че-

рез шлюз, не должен подвергаться проверке и, следовательно, может быть игнорирован администратором простым описанием в политике [30].

Checkpoint IPS — система предотвращения проникновения (IPS). С учетом того, что брандмауэр шлюза безопасности позволяет блокировать потоки данных на основе данных об источнике, пункте назначения и порте, IPS предлагает еще один способ защиты за счет анализа содержания потоков данных с проверкой на предмет наличия риска для сети. IPS защищает как клиентские станции, так и серверы, а также дает возможность контролировать использование сети со стороны определенных приложений [20]. Гибридный модуль обнаружения системы предотвращения проникновения предлагает множество уровней защиты, который предоставляют превосходные возможности по защите и предотвращению известных угроз, а также во многих случаях атак.

Уровни защиты модуля IPS включают:

- обнаружение и профилактика характерных известных атак;
- обнаружение и профилактика уязвимостей, в том числе известных средств атак, например, защита от характерных «Типичных уязвимостей и атак» (Common Vulnerabilities and Exposures — CVE), как изображено на рисунке 6;
- обнаружение и профилактика несанкционированного использования протоколов, что во многих случаях означает вредоносные действия или потенциальную угрозу. Как правило в этих целях используются протоколы HTTP, SMTP, POP и IMAP;
- обнаружение и профилактика входящих вредоносных потоков данных;
- обнаружение и профилактика характерных видов атак без определенных сигнатур, такое как система защиты от вредоносных кодов;

- обнаружение и профилактика попыток туннелирования. Эти попытки могут означать утечку данных или попытки обхода ограничений безопасности, такие как сетевая фильтрация;
- обнаружение, профилактика и наложение ограничений на определенные приложения, которые во многих случаях потребляют много ширины полосы канала или могут стать причиной угроз безопасности для сети, такие как одноранговые локальные вычислительные сети (ЛВС) и приложения обмена мгновенными сообщениями.

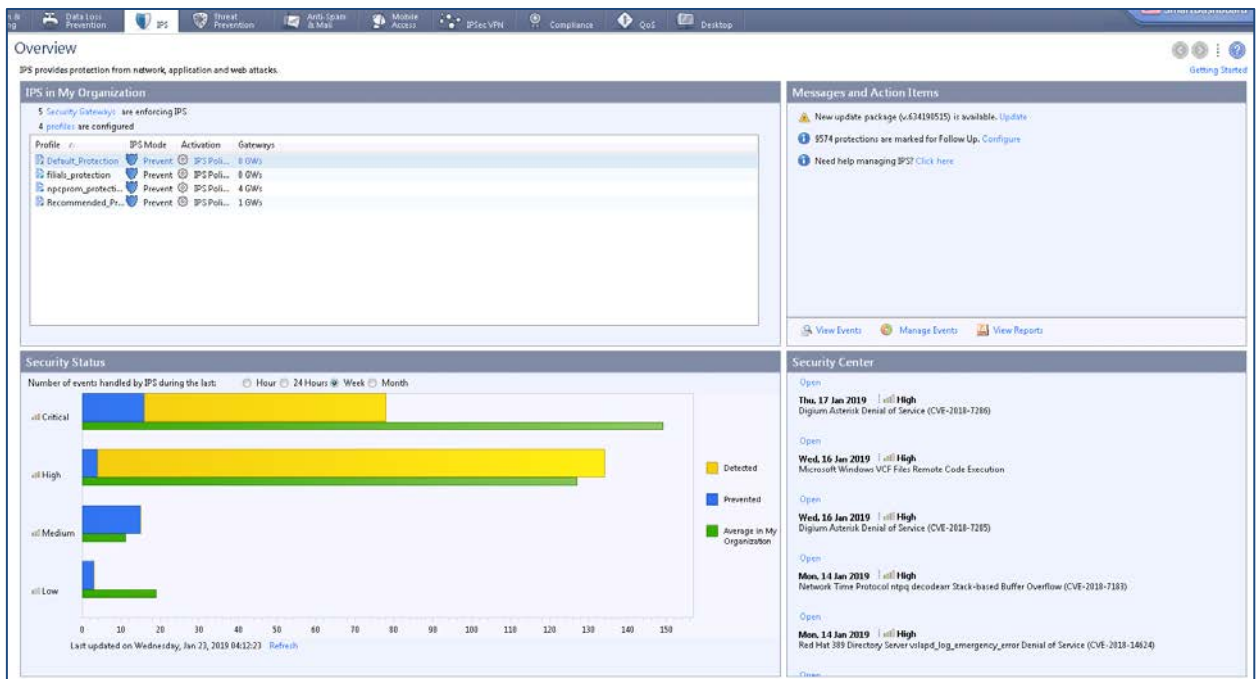


Рисунок 6 — Внешний вид Intrusion Prevention System Блейда

В общем, IPS полностью охватывает десятки протоколов с тысячами видов защиты. Компания Checkpoint постоянно производит обновление библиотек средств защиты, дабы всегда быть готовой к отражению любых угроз.

Модуль системы предотвращения проникновений Checkpoint включает в себя:

- ясный и простой интерфейс управления;
- снижение непроизводительных затрат управления за счет использования одной консоли управления для всех продуктов Checkpoint;

- единая система управления как для сенсоров IPS-1 (IPS-1 Sensors), так и для встроенного программного блейда IPS (IPS Software Blade);
- удобная навигация из окна обзора бизнес-уровня до пакетного захвата при одиночной атаке;
- производительность до 15 Гбит/сек при оптимизированном уровне защите и до 2,5 Гбит/с при задействовании всех средств защиты IPS;
- приоритетный охват системой безопасности уязвимостей программного обеспечения Microsoft и Adobe. Регулировка использования ресурсов с тем, чтобы высокая активность IPS не отражалась на прочих функциях программного блейда.

Полная интеграция с инструментами конфигурирования и мониторинга Checkpoint, такими как SmartEvent, SmartView Tracker и SmartDashboard, позволяющая принимать незамедлительные меры на основе информации IPS.

Mobile Access Blade — является наиболее полным решением для надежного подключения мобильных сотрудников, удаленно работающих сотрудников, временных работников и внешних партнеров к необходимой им информации [25]. Для подключения удаленных работников есть несколько вариантов опций, которые снижают затраты компании на администрирование. Решение обеспечивает удаленный доступ корпоративного уровня через Интернет при помощи смартфона, планшета или ПК, как через VPN 3-го уровня, так и SSL VPN, предоставляя вам простую, безопасную и надежную связь с электронной почтой, календарем, контактами и корпоративными приложениями [26].

Основные свойства блейда:

- безопасный доступ по SSL VPN;
- свухфакторная аутентификацию;
- соответствие Устройство/Конечный пользователь на основе сертификатов;
- мобильный бизнес-портал;

- интеграция с дополнительными программными блейдами шлюза безопасности включая IPS, Anti-malware и Firewall.

Клиент Checkpoint Mobile наиболее подходящий способ для простого и безопасного подключения к корпоративным ресурсам со смартфонов и ПК.

Защищенный бизнес-портал настроен для каждого пользователя и гарантирует доступ только к разрешенным корпоративным ресурсам.

Технология SSL VPN используется для надежного шифрования данных при передаче информации между мобильными устройствами и корпоративной ИТ-инфраструктурой. Доступ как на уровне Web-интерфейса, так и на сетевом уровне, может быть реализован посредством SSL-шифрования через практически любой интернет-браузер.

Программный блейд **Identity Awareness** — обеспечивает интеграцию Microsoft Active Directory (AD) пользователей, групп и устройств, а также контроль доступа через создание политики на основе идентификации пользователя AD. Данный функционал по умолчанию входит во все устройства Checkpoint и позволяет в политиках использовать учетные записи и\или группы пользователей AD [17].

Возможности блейда Identity Awareness:

- централизованное управление доступом пользователей к ресурсам компании и интернет-приложениям;
- возможность применения индивидуальной политики для каждого пользователя/ группы/ устройства AD;
- простота определения пользователей — сотрудников компании или других лиц (гостей и подрядчиков);
- индивидуальный доступ к центрам обработки данных, приложениям и сетевым сегментам для пользователей, отделов или устройств;
- предотвращение несанкционированного доступа к ресурсам, совмещенное с возможностью удаленной работы;

- предотвращение угроз и потери данных путем ограничения доступа к ресурсам для пользователей и устройств;
- централизованное управление и мониторинг позволяют управлять политикой посредством единой консоли;
- интеграция Identity Awareness в архитектуру программных блейдов CheckPoint;
- обеспечение масштабируемого обмена данными об аутентификации пользователей между шлюзами;
- Identity Awareness Software Blade обеспечивает несколько способов получения идентификационных данных пользователя, включая: AD Query, Browser-Based (через браузер) и IdentityAgents;
- идентификационная информация может использоваться соответствующими программными блейдами для применения индивидуальной политики [28].

Identity Awareness Software Blade позволяет легко добавлять пользователей, группы и устройства AD для их идентификации, обеспечивая тем самым безопасность вашей компании и удобство построения политик безопасности, образец показан на рисунке 7.

Identity Awareness Software Blade обеспечивает несколько способов получения идентификационных данных пользователя, включая: AD Query, Browser-Based (через браузер) и Identity Agents.

Идентификационная информация может использоваться соответствующими программными блейдами для применения индивидуальной политики.

AD Query — запрос к контроллерам домена. Легко разворачиваемый, основанный на интеграции с Active Directory, полностью прозрачный для пользователя.

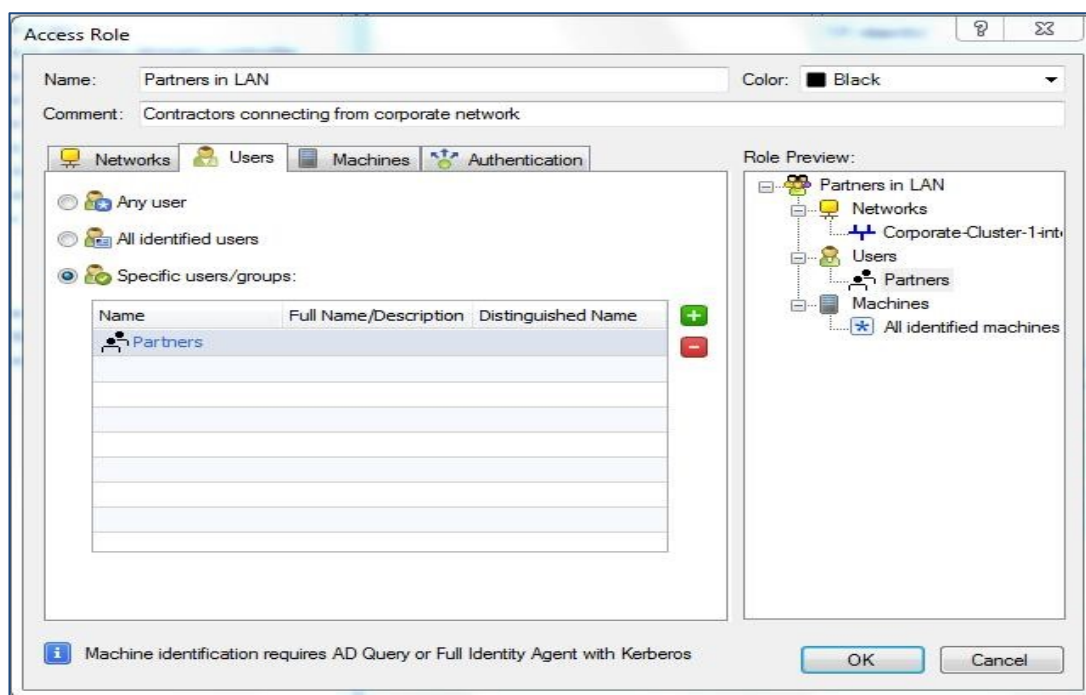


Рисунок 7 — Добавление пользователей

Browser-Based Authentication — проверка подлинности на основе браузера. Для обеспечения идентификации неизвестных пользователей Вы можете использовать следующие методы:

1. Captive Portal — простой метод, заключающийся в проверке подлинности пользователей через Web-интерфейс до предоставления ему доступа к ресурсам внутренней сети. Когда пользователь пытается получить доступ к защищенному ресурсу, он переходит на Web-страницу, в которой необходимо заполнить поля логин и пароль для дальнейшей работы.

2. Transparent Kerberos Authentication — «прозрачная» проверка подлинности пользователей посредством браузера, включающая проверку информации о личности до открытия им страницы имени пользователя / пароля в Captive Portal. При настройке этого параметра Captive Portal запрашивает данные аутентификации из браузера. После успешной аутентификации пользователь перенаправляется к своей первоначальной цели. Если проверка не прошла, пользователь должен ввести учетные данные в Captive Portal.

3. Identity Agents — агент на ПК или терминальный сервер. Данный метод требует установки агента на машину пользователя. Два типа Identity Agents:

- Endpoint Identity Agents — специализированные клиентские агенты, установленные на компьютерах пользователей, которые задают и передают идентификационные данные на шлюз безопасности Security Gateway;
- Terminal Servers Identity Agent — агент, установленный на терминальном сервере приложений, где размещены сервисы Citrix / MS Terminal. Там и происходит идентификация пользователей, использующих в качестве источника общий IP-адрес сервера.

4. Использование Endpoint Identity Agents идентифицирует пользователей и устройства, все необходимые настройки выполняются администратором и не требуют ввода данных пользователем.

Кроме этого, Identity Agents позволяют:

1. Подключаться через роуминг — пользователи остаются идентифицированными, даже когда перемещаются между сетями, так как клиент обнаруживает данные перемещения и подключения.

2. Повышенная безопасность — можно использовать запатентованную технологию «packet tagging» для предотвращения подмены IP-адресов. Endpoint Identity Agents также дает возможность надежной аутентификации пользователей и устройств через Kerberos.

3. RADIUS Accounting — идентификация на базе RADIUS сервера. Она получает идентификационные данные пользователей из запросов, которые генерируются клиентом RADIUS. Identity Awareness использует данные из этих запросов для получения информации о пользователях и группе устройств с сервера LDAP.

4. Удаленный доступ (VPN SSO) — идентификация доступна для удаленного пользования через мобильные устройства и IPSec VPN, настроенных на работу в офисном режиме Office Mode и в случае подключения к шлюзу Security Gateway.

С помощью них есть возможность:

- узнать о приложениях, для этого можно использовать исчерпывающую базу данных AppWiki от Checkpoint, чтобы получить представление о том, какие приложения используются и каковы их уровни риска (рисунок 9) [16];

- создать детальную политику — создание правил пропуска или блокировки приложений или интернет-сайтов по отдельному приложению, категориям приложений или URL или по уровням риска. При использовании Identity Awareness вы можете легко устанавливать правила для отдельных пользователей или разных групп пользователей. Вы также можете создать политику HTTPS, позволяющую шлюзу проверять HTTPS трафик во избежание рисков для безопасности, связанных с SSL-протоколом;

- узнать, что делают сотрудники предприятия — использование SmartViewTracker и SmartEvent позволяет видеть трафик приложений и сайтов, реально существующий в среде компании. Только администраторы, имеющие соответствующие разрешения, могут видеть все поля в журнале. Использование разрешений обеспечивает конфиденциальность секретных данных в журналах и невозможность их просмотра всеми администраторами;

- поддерживать актуальность политик — база данных Application and URL Filtering регулярно пополняется категориями приложений и сайтов для поддержания актуальности политики. Шлюз устанавливает соединение с онлайн Web-службой Checkpoint для идентификации виджетов социальных сетей и категорий Web-сайтов для нераспознанных URL. Результаты сохраняются в локальный кэш на каждом шлюзе безопасности. В дальнейшем некатегоризованные URL перед отправкой запроса в онлайн Web-службу Checkpoint проверяются в местном кэше;

- настраивать приложения, сайты, категории и группы — есть возможность создавать приложения, Web-сайты, категории и группы, отсутствующие в базе данных Application and URL Filtering, для использования в по-

литике. Использовать пользовательские объекты для создания базы правил, соответствующей требованиям организации.

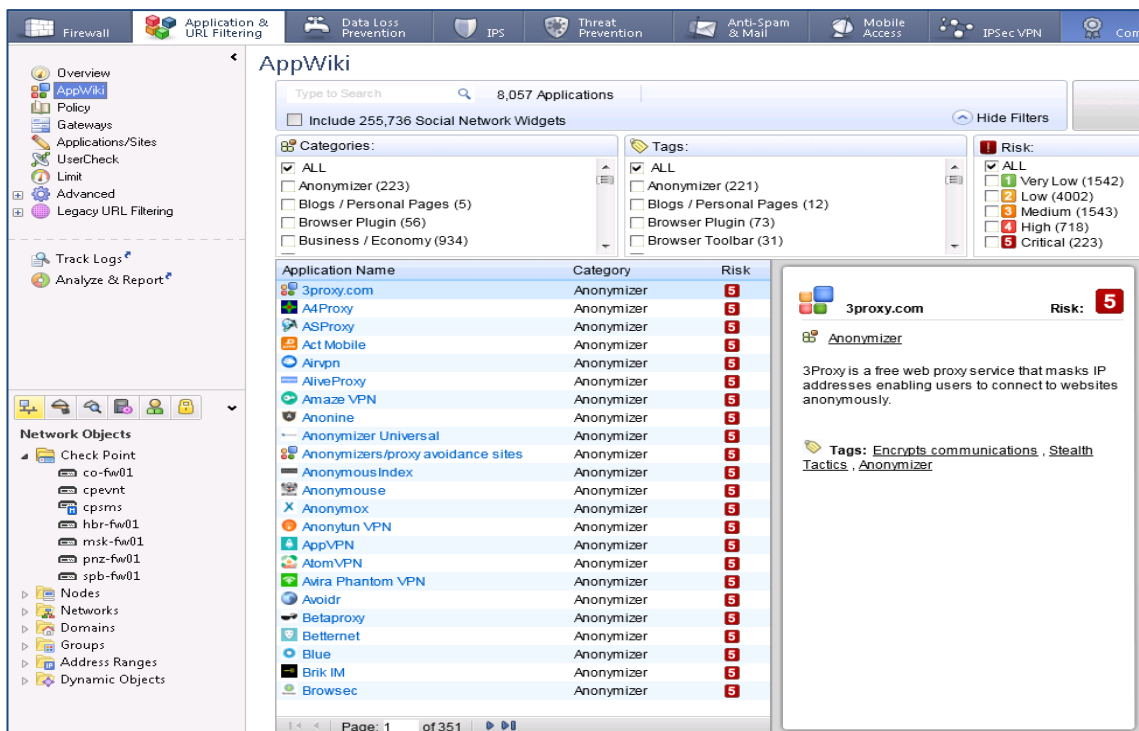


Рисунок 9 — AppWiki

Кроме того, можно обратиться к Checkpoint на предмет создания сигнатур специализированных приложений для последующего импорта в базу данных. Этот файл может содержать, например, базу данных с внутренними приложениями организации, причем необязательно с использованием Web-технологий [16].

1.5 Определение руководства администратора и требования к его реализации

Документ «Руководство администратора» относится к пакету эксплуатационной документации. Основная цель руководства заключается в обеспечении пользователя необходимой информацией для самостоятельной работы с программой или автоматизированной системой [6].

Следовательно, документ «Руководство администратора» (далее руководство администратор) должен отвечать на следующие вопросы: что это за

программа, что она может, что необходимо для обеспечения ее корректного функционирования и что делать в случае отказа системы.

Как правило, руководство администратор состоит из:

- описания системы;
- администрирования компонентов системы;
- приложения.

В разделе «Описание системы» указываются состав и функции компонентов системы, а также структура программного обеспечения.

В разделе «Администрирование компонентов системы» в нашем случае описывается порядок развертывания компонентов системы, их настройка, регламентные работы и устранение возможных неполадок.

В «Приложениях» обычно указывается уточняющая информация, например, схема системы и ее IP-адресация.

Руководство администратора должно представлять собой краткий справочник по основному функционалу системы или развернутое учебное пособие. Методы изложения материала в данном случае будет зависеть от функционала информационной системы [8].

Чем подробнее будут описаны действия с системой, тем меньше вопросов возникнет у пользователя. Для более легкого понимания всех принципов работы с программой стандартами в документе «Руководство администратора» допускается использовать схемы, таблицы, иллюстрации с изображением экранных форм.

В качестве аналогов были проанализированы нижеследующие руководства.

Руководство администратора «Подсистемы распределенного аудита и управления «Аккорд-РАУ» [1]. Содержание этого руководства, изображенное на рисунке 10, очень подробное и содержит нумерацию, что облегчает поиск информации. Оно разбито на главы, что создает некую последовательность для изучения.

Содержание

1	Содержание работы администратора безопасности информации	4
1.1	Планирование применения комплекса "Аккорд"	4
1.2	Установка и настройка комплекса "Аккорд"	5
1.3	Эксплуатация комплекса	5
2	Эксплуатация автоматизированного рабочего места администратора безопасности информации (АРМ АБИ)	6
2.1	Общий вид АРМ администратора безопасности	6
2.2	Общий вид панели управления	7
2.3	Меню команд	7
	Поиск клиентов в сети	7
	Получить информацию о станциях	7
	Установить уровень детальности журнала	8
	Заблокировать станции	8
	Разблокировать станции	8
	Послать сообщение станциям	8
	Получить экран станции	8
	Отключить станцию	8
	Получить журналы от станций:	9
	Разослать список станций	9
	Получение и редактирование файлов конфигураций станции	9
	Проводник сети "Аккорд"	10
	Синхронизация баз пользователей	10
	Редактирование базы пользователей	10
	Очистка окон	11
2.4	Сообщения программы	13

Рисунок 10 — Оглавление руководства «Подсистемы распределенного аудита и управления «Аккорд-РАУ»»

На рисунке 11 представлено изображение, которое используется в руководстве администратора «Подсистемы распределенного аудита и управления «Аккорд-РАУ»». Этот рисунок представляет окно приложения, правда функционал отдельно взятой строки не описывается, похоже идет расчет на интуитивную понятность интерфейса. Данное представление содержания является удобным для поиска информации, но затрудняет восприятие картины в целом, а выделение в виде стрелок или описание функционала каждой отдельно взятой строки было бы более наглядным. Однако данное содержание распространяется в формате PDF, т.е. не обладает такими интерактивными элементами, как, например, поиск, навигация и гиперссылки.

Редактирование базы пользователей

Администратор может редактировать базы пользователей на АРМ. Измененные базы рассылаются пользователям после редактирования. После выбора этой команды открывается окно редактора ПРД, практически такого же, как в локальной версии. Единственное отличие – вместо пункта контроля целостности установка временного интервала перезагрузки станции после получения новой базы пользователей.

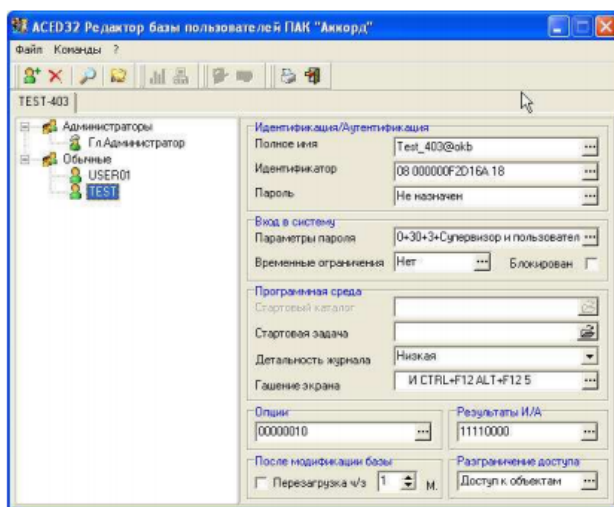


Рисунок 11 — Окно руководства «Подсистемы распределенного аудита и управления «Аккорд-РАУ»»

Руководство администратора «JaCarta SecurLogon» также, как и предыдущее рассматриваемое руководство содержит нумерацию и четкую структуру в содержании, это изображено на рисунке 12 [10].


JaCarta SecurLogon Руководство администратора			
<h2>Содержание</h2>			
1.	Введение		3
1.1.	Общие сведения		3
1.2.	Дополнительная документация.....		3
2.	Системные требования.....		4
3.	Установка лицензии SecurLogon		5
3.1.	Установка лицензии на локальном компьютере		5
4.	Административный шаблон из состава SecurLogon.....		9
4.1.	Доступ к настройкам административного шаблона		9
4.2.	Настройки административного шаблона SecurLogon		12
5.	Операции с профилями SecurLogon		16
5.1.	Создание профиля SecurLogon.....		16
5.2.	Установка профиля по умолчанию		20
5.3.	Редактирование существующего профиля SecurLogon		21
5.4.	Удаление профиля SecurLogon		22
	Лист регистрации изменений.....		25

Рисунок 12 — Содержание руководства «JaCarta SecurLogon»

Так же хорошо оформлены возможности политики управления. В таблице, изображенной на рисунке 13, подробно предоставлено описание и возможности различных функций программы. И отлично представлены сноски-подсказки с особенностями моментами.

4.2. Настройки административного шаблона SecurLogon

Табл. 2

Политики управления SecurLogon

Название	Описание	Допустимые значения	Значение по умолчанию до распространения групповых политик ¹	Значение по умолчанию в шаблоне ²
AdditionalDomains (Дополнительные домены)	Список дополнительных доменов, отображаемых при создании профиля или при входе с использованием профиля SecurLogon.	<ul style="list-style-type: none"> Имена доменов Windows, указанные через точку с запятой; пустая строка. 	Пустая строка	Пустая строка
AllowProfileManagement (Разрешить создание профилей пользователями)	Разрешает или запрещает пользователю создавать профили SecurLogon	<ul style="list-style-type: none"> Не задано – будет использоваться значение по умолчанию, заданное в шаблоне (последний столбец настоящей таблицы); Включено – пользователи могут самостоятельно создавать профили; Отключено – пользователи не могут самостоятельно создавать профили. 	Включено	Отключено
AllowedLogonMethods (Разрешённые методы аутентификации)	Определяет перечень доступных методов аутентификации, которые доступны для входа в операционную систему.	<ul style="list-style-type: none"> Не задано – будет использоваться значение по умолчанию (последний столбец настоящей таблицы); Отключено – будут использоваться стандартные механизмы Windows; Включено – позволяет явно задать, какие методы входа можно будет использовать (при этом значение 1 означает, что метод разрешён, а 0 - запрещён); Примечание: если все методы входа имеют одинаковые значения (как 0, так и 1), это означает, что все эти методы разрешены. DefaultPasswordLogon – стандартный 	Выбраны все методы	Выбраны все методы

¹ Эти значения применяются сразу после установки Единого Клиента JaCarta

² Применяются после распространения групповых политик, если в административный шаблон SecurLogon не было внесено никаких изменений

V1.0 31.10.2014 стр.12 из 25

Рисунок 13 — Таблица политики управления руководства «JaCarta SecurLogon»

Представленные выше руководства администратора являются официальными руководствами от производителей предоставляемых ими программ. Они имеют схожую структуру, имеются разделы по установке программного обеспечения, настройке, администрированию, но ни одно из рассматриваемых руководств не имеет раздела по устранению типичных или возможных неполадок в работе. Руководства пользователя снабжены большим количеством иллюстрациями, а сами иллюстрации содержат указатели на описываемый элемент. Органично выглядят вставки примечаний, советов и важных моментов. Тем не менее, все они распространяются в формате PDF, т.е. не обладают такими интерактивными элементами, как, например, поиск, навигация и гиперссылки.

Тем не менее, ни один из рассмотренных руководств не может послужить примером для разрабатываемого руководства ввиду разного содержания систем.

1.6 Выбор программных средств, для реализации руководства администратора

Прежде чем перейти к непосредственному созданию электронного пособия необходимо ознакомиться и проанализировать доступные программные средства для создания электронных методических материалов, чтобы выбрать наиболее подходящие.

Dr.Explain 5.3 — полуавтоматические руководства с готовыми аннотациями [18]:

- разработчик: Indigo Byte Systems;
- операционная система: Windows;
- распространение: shareware, от 7 500 рублей;
- русский интерфейс: есть.

Dr.Explain не может похвастаться таким современным интерфейсом, как Clarify, представленным на рисунке 14, однако у этой программы есть свои уникальные особенности. Пожалуй, самое главное — это автоматизация процесса создания технической документации. Просто укажите окно приложения или же Web-страницу сервиса, которые нужно описать, и Dr.Explain самостоятельно создаст скриншот, проанализирует все элементы интерфейса, добавит выноски и даже подпишет их там, где это возможно.

Программа способна анализировать пользовательский интерфейс приложений и создавать скриншоты (копии экранов) окон, автоматически расставляя на них пояснительные выноски для элементов интерфейса.

Процесс практически полностью автоматизирован, что позволяет достаточно быстро аннотировать экраны приложений и Web-сайтов для иллюстрирования пользовательской документации на ПО.

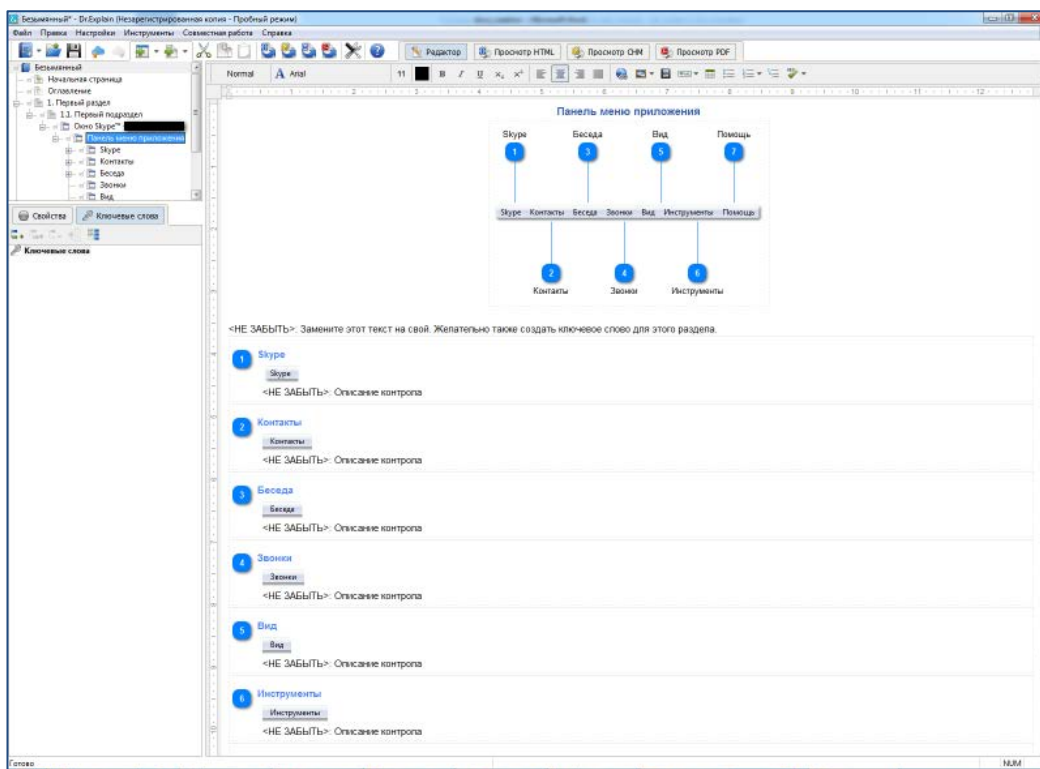


Рисунок 14 — Окно программы Dr.Explain

Для экспорта готовой документации предлагаются форматы CHM, DOC, HTML и PDF. При этом еще до выполнения экспорта можно увидеть, как мануал будет выглядеть в одном из этих форматов. Наконец, стоит обратить внимание на то, что Dr.Explain — продукт отечественных разработчиков, поэтому вполне ожидаемо, что в нем можно найти полноценную поддержку русского языка.

Natata eBook Compiler — программа для создания электронных книг на основе скачанных сайтов или специально подготовленных наборов HTML страниц с картинками. Поддержка HTML, CSS, WAV, TXT, GIF, JPG, MID, javascript, DHTML, Flash, PDF, DOC и других форматов. Объединяет все страницы единой оболочкой, позволяющей ограничить количество просмотров книги, доступ к HTML коду. С помощью Natata eBook Compiler возможно создать: электронную книгу; цифровой каталог; корпоративный проект; электронный журнал; offline Web-сайт; руководство пользователя; портфолио; маркетинговую презентацию; учебно-образовательный материал [27]. Интерфейс программы представлен на рисунке 15.

При этом руководство пользователя смотрятся одинаково хорошо на любых устройствах — на больших мониторах, планшетах или смартфонах. Сервис автоматически выполняет адаптацию под размер экрана.

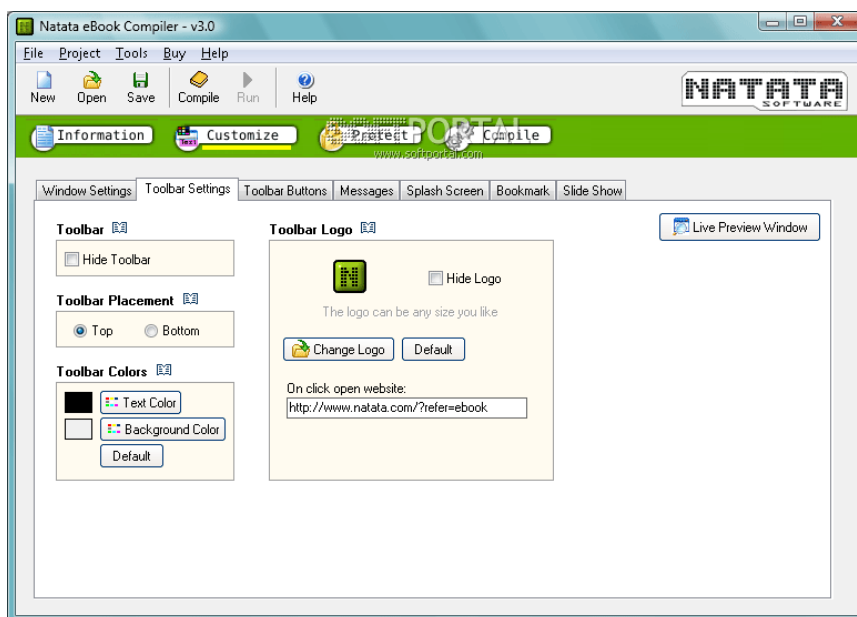


Рисунок 15 — Окно программы Natata eBook Compiler

Процесс создания книги состоит в заполнении вкладок, что позволяет шаг за шагом указать все необходимые параметры будущей книги, включая возможность выбрать уровень сжатия. В бесплатной версии для сборки книги можно использовать популярные текстовые, графические и аудио форматы, но нельзя включить в книгу Flash, PDF или, к примеру, DOC, DOCX — для этого придется купить версию Pro или Gold. Кроме этого, ограничены опции по защите книги — доступен только запрет на копирование и печать, а вот пароль на книгу поставить нельзя.

Недостатками данной программы являются интерфейс на английском языке, отсутствие доступа к файлам PDF, невозможность выполнения ссылок на файлы с расширением EXE.

HelpNDoc — простая в использовании и очень удобная программа для создания справочной документации в различных форматах: стандартном СНМ, Web-документации, файлах PDF или DOC, DOCX [23]. HelpNDoc обладает всеми необходимыми возможностями, которые помогут как опытным пользователям, так и новичкам. Программа бесплатна для персонального ис-

пользования. Назначение HelpNDoc — создание справоч. Интерфейс изображен на рисунке 16.

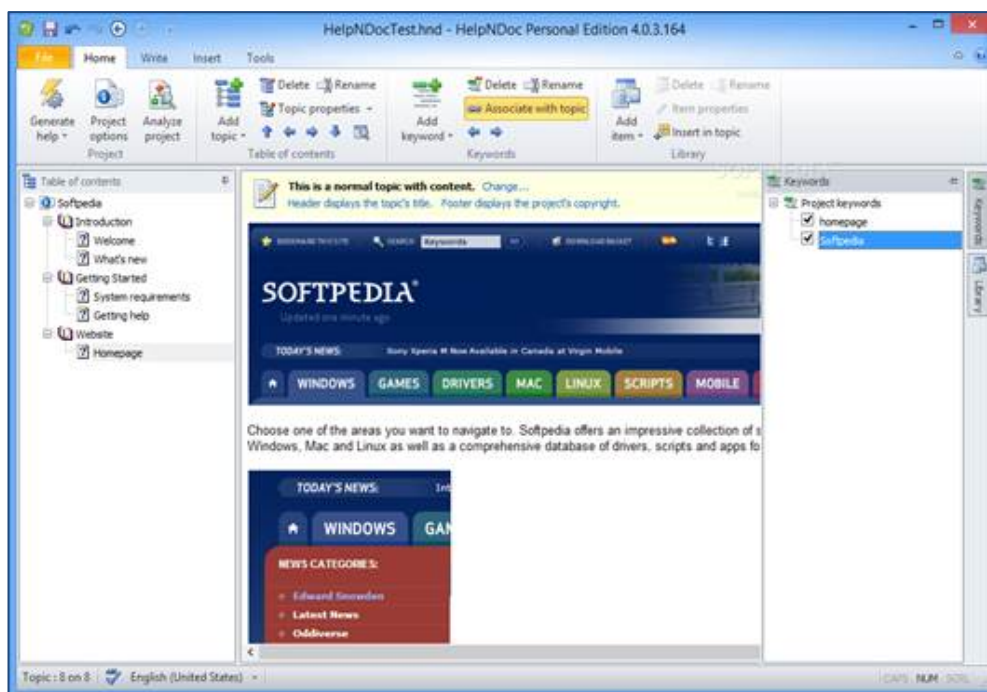


Рисунок 16 — Окно программы HelpNDoc

Интерфейс последней версии сделан по типу интерфейса программ Microsoft Office — меню и панели инструментов заменили вкладки. В программе четыре постоянные вкладки и несколько дополнительных. Вкладки содержат необходимые команды для разных видов работы: для формирования и оформления списка тем справки, для создания и оформления текста, для вставки различных объектов и пр. Созданная справка преобразуется в 4 формата: в файлы Chm, DOC, HTML, PDF.

Для создания справки в формате HTML редактор использует фреймы (рамки), раскрывающий список и JavaScript. Но так как вся работа ведется в визуальном режиме, то пользователь может забыть и о фреймах, и о JavaScript — при работе это ему не понадобится. HelpNDoc заменил всю эту премудрость заранее заготовленными шаблонами, с использованием которых и создается справка. Кроме этого, в программе есть ряд мастеров для разных операций.

Составной частью HelpNDoc является хороший визуальный редактор Web-страниц. Редактор позволяет вставить на страницу текст, изображения, таблицы, различные символы, отсутствующие на клавиатуре, ссылки, списки, видео и др. В программе имеется библиотека, позволяющая хранить тексты, изображения, видео, отрывки кода HTML и другое.

SunRav BookOffice — пакет, состоящий из двух программ, окна которых представлены на рисунке 17: SunRav BookEditor — программа для создания и редактирования книг и учебников и SunRav BookReader — программа для просмотра книг и учебников [7].

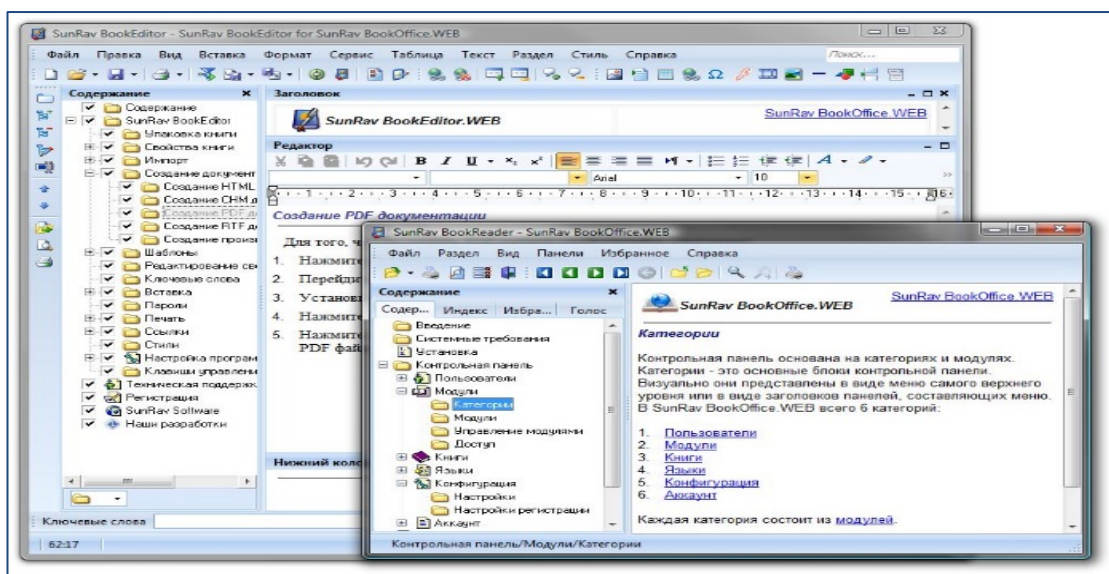


Рисунок 17 — Окна программ SunRav BookEditor и BookReader

С помощью программы SunRav BookEditor можно создать: электронные книги, учебники, электронные словари или энциклопедии; HTML, CHM и PDF документы, документы в произвольном формате (с помощью шаблонов). Программа позволяет компилировать книги в EXE файлы и имеет следующие особенности:

- возможность определить различные стили текста и с их помощью очень быстро форматировать текст;
- проверка орфографии позволяет проверять правописание на ходу;
- разнообразные таблицы, в том числе вложенные друг в друга;

- импорт всех документов из одной папки с автоматическим созданием разделов, а также импорт книг из СНМ файлов;
- импорт и экспорт книг из (в) файлы MS Office: DOC, XLS и т.д.;
- ссылки облегчают навигацию по книге, запускают различные документы и программы, имеется возможность открытия ссылок во всплывающих окнах;
- «ленточный» интерфейс аналогичный интерфейсу программ Microsoft Office 2007–2013;
- вставка изображений, видео, аудио файлов, специальных символов, роликов YouTube, Flash и GIF;
- быстрый просмотр созданной книги в программе SunRay BookReader.

Рассмотрев и проанализировав представленные выше программные продукты, выбор был совершен в пользу Dr.Explain, так как у выбранного программного продукта нет ограничений по времени в бесплатной версии и есть поддержка русского языка, а также присутствует полуавтоматическая система, упрощающая разработку.

2 РАЗРАБОТКА ЭЛЕКТРОННОГО РУКОВОДСТВА АДМИНИСТРАТОРА ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА CHECKPOINT

2.1 Цель и назначение руководства администратора программно-аппаратного комплекса

Поскольку необходимо, чтобы каждый пользователь комплекса максимально четко и ясно представлял, какие действия необходимо выполнить для реализации поставленной задачи, то задачу по наполнению разрабатываемого руководства нужно проработать и изучить как можно лучше. Нужно проанализировать все повседневные действия, такие как создание разрешающих правил, реакция на инциденты, создание отчетов, обновление баз и т.п.

Основная задача руководства состоит в том, чтобы обеспечить пользователям возможность самостоятельно решать все основные задачи, на которые нацелена система.

Данное руководство будет использоваться администраторами программно-аппаратного комплекса Checkpoint, для обеспечения информационной безопасности предприятия НПЦ «Промэлектроника».

АО «НПЦ “Промэлектроника”» — предприятие, основным видом деятельности которого является разработка систем безопасности движения поездов на магистральных железных дорогах, подъездных путях промышленных предприятий и в метрополитене [5].

За работоспособность всей сетевой инфраструктуры предприятия отвечает отдел информационных технологий, в который входят группы информационных систем, технической поддержки, автоматизации и специалист по информационной безопасности.

Доступ к администрированию программно-аппаратного комплекса Checkpoint имеет лишь специалист по информационной безопасности и руководитель группы информационных систем.

А так как вся имеющаяся документация для комплекса лишь на английском языке, то для того, чтобы каждый из имеющих доступ к комплексу мог полноценно выполнять необходимые задачи по администрированию необходимо будет создать руководство, но только после перевода функционала.

Разрабатываемое руководство администратора будет служить основой для изучения конфигурации, а также справочным материалам по часто стандартным процедурам и аварийным ситуациям.

2.2 Общее описание структуры и интерфейса руководства администратора

Проектирование руководства начинается с определения его структуры и содержания [1, 5].

В соответствии с требованиями к разрабатываемому руководству, исходя из которых администратор программно-аппаратного комплекса должен уметь производить первоначальную настройку оборудования, начиная с установки операционной системы, заканчивая подключением к центральному шлюзу Checkpoint, устанавливая обновления программного обеспечения на компоненты, создавать резервные копии, продлевать или привязывать необходимые лицензии, а также устранять возможные неполадки. Руководство администратора программно-аппаратного комплекса Checkpoint сгруппировано по типам описываемых в них инструкций:

1. Описание системы.
2. Администрирование компонентов системы.
 - 2.1. Порядок развертывания компонентов системы.
 - 2.2. Настройка компонентов системы.

2.3. Регламентные работы.

2.4. Устранение возможных неполадок.

3. Приложение.

Выбор компонентов руководства основывался на текущих и часто используемых задачах в процессе эксплуатации программно-аппаратного комплекса Checkpoint, а так же исходя из имеющихся в открытом доступе источников, в которых решаются нестандартные ситуации работы комплекса.

Каждая глава руководства разбита на вкладки, в которых конкретно объясняется каждое действие для выполнения поставленной задачи, кроме того, для удобства навигации в меню, в каждой вкладке были выделены дополнительные разделы, в которых рассматривается конкретная ситуация. Данное решение позволяет тратить в разы меньше времени на поиск необходимой информации.

Dr.Explain — программа для создания руководства, рассмотренная выше, имеет пробную версию, ограничения которой это водные знаки на изображениях, которые, однако не мешают изучению конфигурации и созданию руководства [22].

На главной странице программы, представленной на рисунке 18, расположены кнопки создания, открытия и импорта проекта.

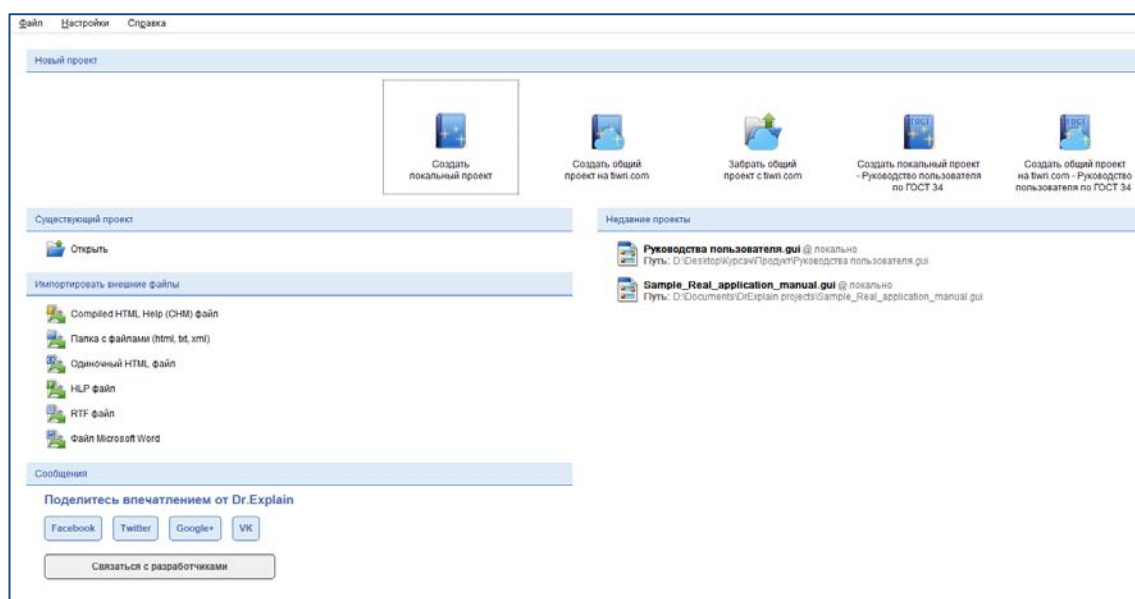


Рисунок 18 — Начальная страница программы Dr.Explain

При создании нового проекта, первое, что необходимо выбрать вид создаваемого руководства, как представлено на рисунке 19.

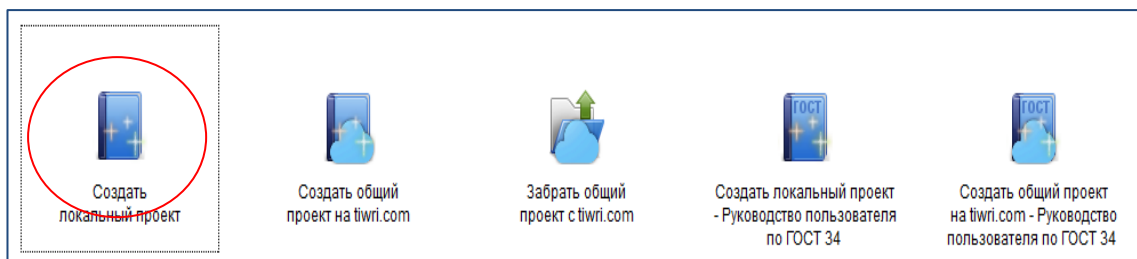


Рисунок 19 — Создание проекта

В нашем случае был выбран локальный проект, в котором можно задать необходимую структуру для будущего руководства.

После создания проекта открылось начальное окно, со стандартной структурой, представленная на рисунке 20 [11].

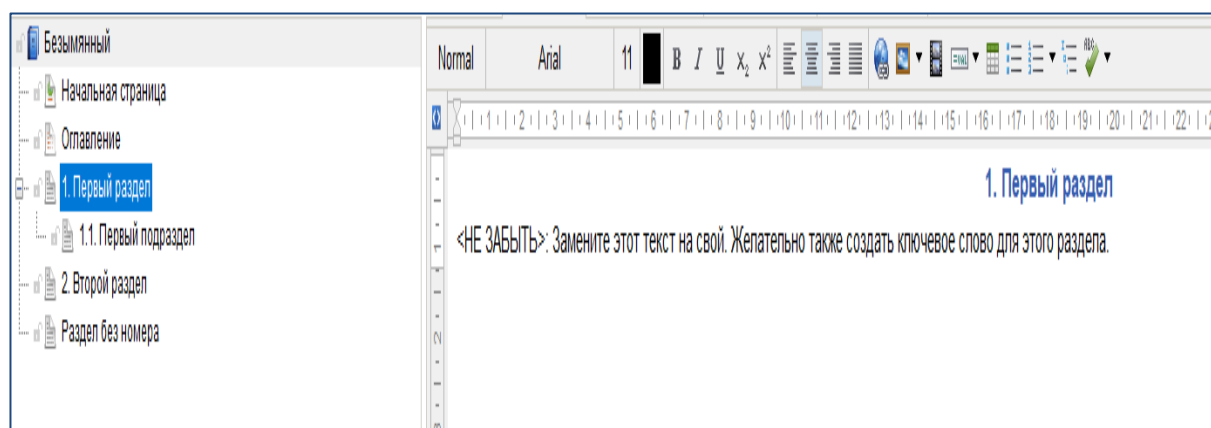


Рисунок 20 — Окно проекта с сформированной структурой

Для наполнения проекта данными и материалами была проработана структура документа, основываясь на основных задачах, которые потребуются выполнять сотрудникам, выполняющих обязанности администратора комплекса, например, первоначальная установка операционной системы (ОС) на новые устройства Checkpoint, реагирования на различные инциденты. Распределения по ролям не будет, т.к. руководство администратора будет предназначено только для тех сотрудников, которые будут работать с аппаратно-программным комплексом.

В итоге была сформирована схема, показывающая уровни вложенности глав и подглав, представленная на рисунке 21.

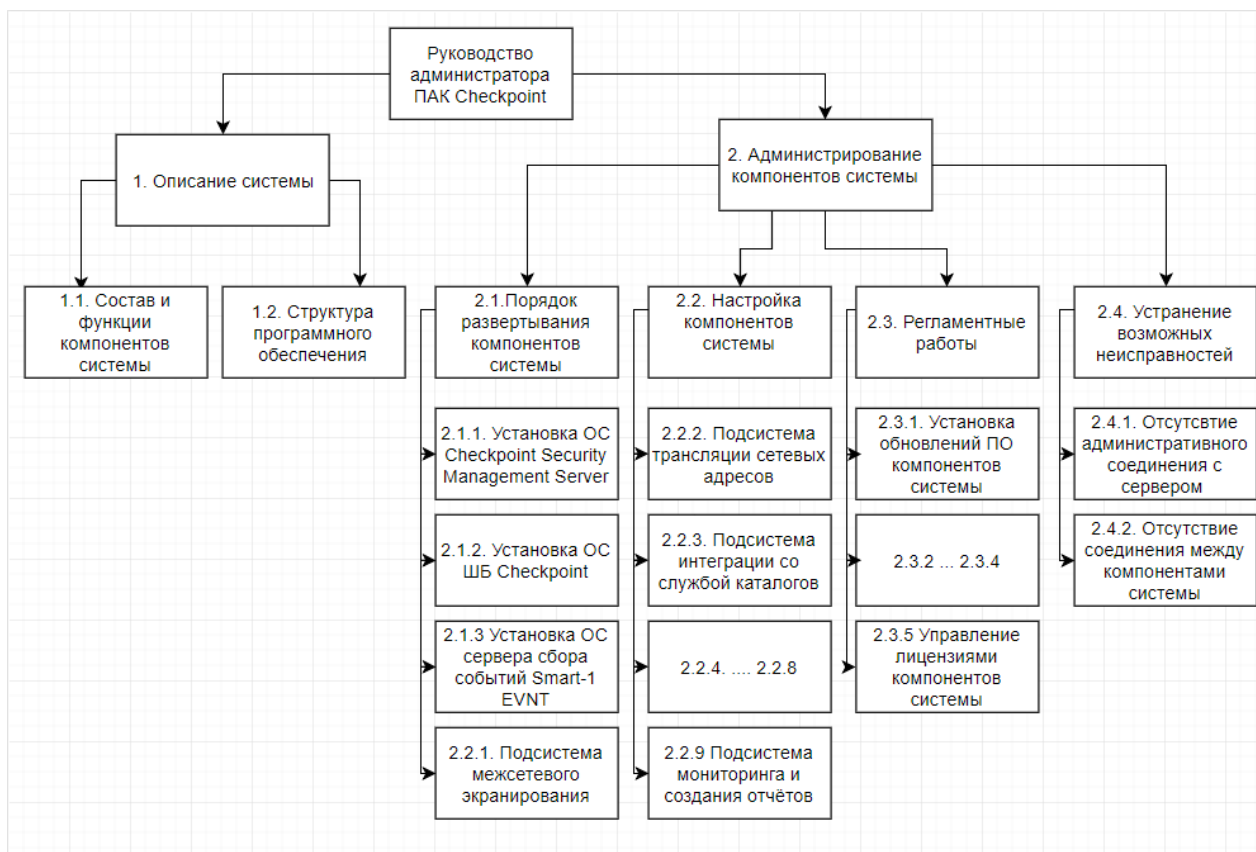


Рисунок 21 — Схема структуры главы «Описание операций»

Схема отражает суть руководства и механизм работы, а также описывает его границы. Создание схемы является одной из самых важных частей описания. Сформированная схема сильно поможет при создании дальнейшей структуры.

После создания структуры необходимо сформулировать набор действий для каждого объекта, которые представляют главы и подглавы, что и было сделано.

Руководство состоит из двух основных глав:

1. Описание системы.
2. Администрирование компонентов системы.

Далее в разделе описание операций была создана описанная выше структура, представленная на рисунке 22, с помощью инструментов добавления, удаления и переходов с уровня на уровень, находящихся в контекстном меню сформированной структуры.

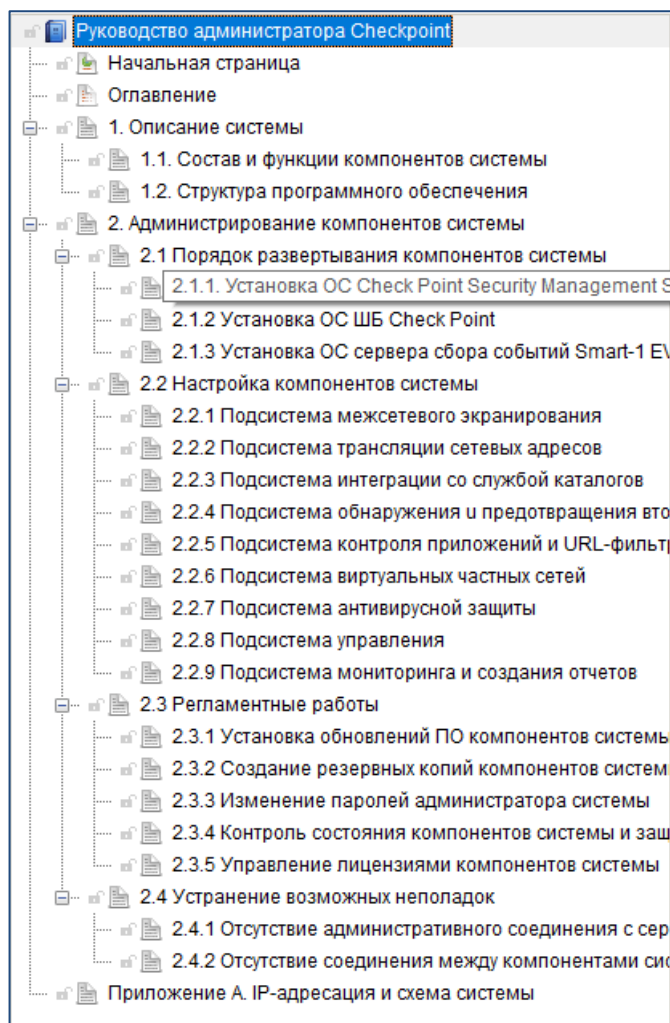


Рисунок 22 — Структура описания операций

Заполнив страницу в окне редактора, можно посмотреть, как будет в итоге выглядеть продукт, образец показан на рисунке 23. А при необходимости поправить стили или шрифты, а так же форматирование текста.

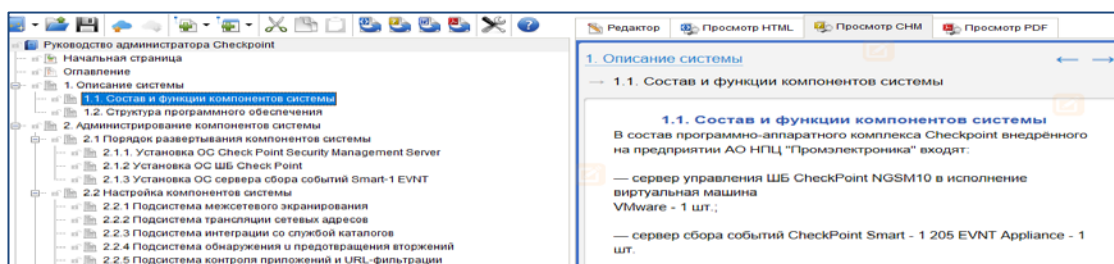


Рисунок 23 — Настройка страницы

Так же был установлен логотип предприятия, как на рисунке 24. Кроме того, в настройках навигации был выбран пункт «Спрятать ссылку на Dr. Explain», для того чтобы убрать лишние ссылки из руководства.

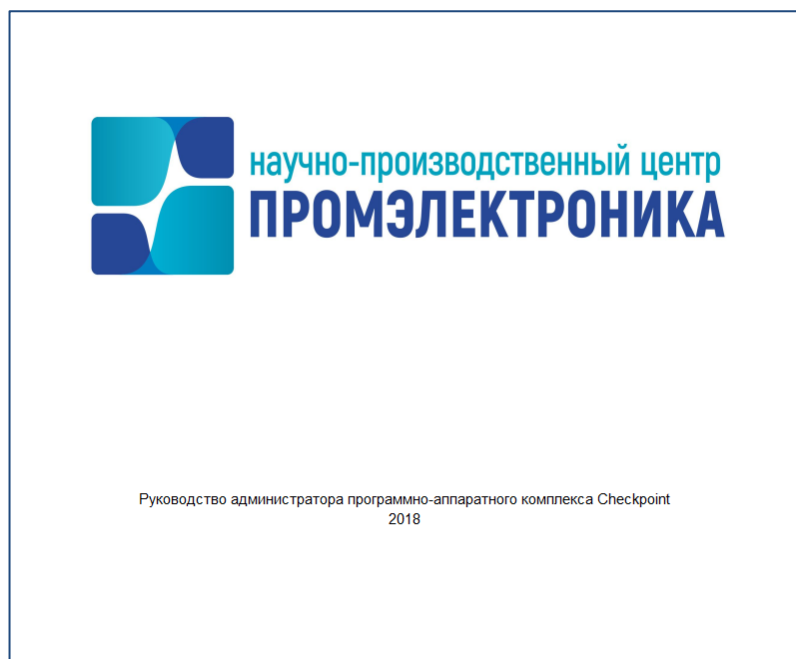


Рисунок 24 — Начальная страница

После настроек проекта и проверки конечного продукта руководство было полностью заполнено.

В процессе заполнения было решено добавить гиперссылки на официальные сайты Checkpoint, для более подробного изучения появившегося вопроса, либо если информация будет не ясна, пример показан на рисунке 25 [24].

Добавление гиперссылок производится также, как и в программе Microsoft Word.

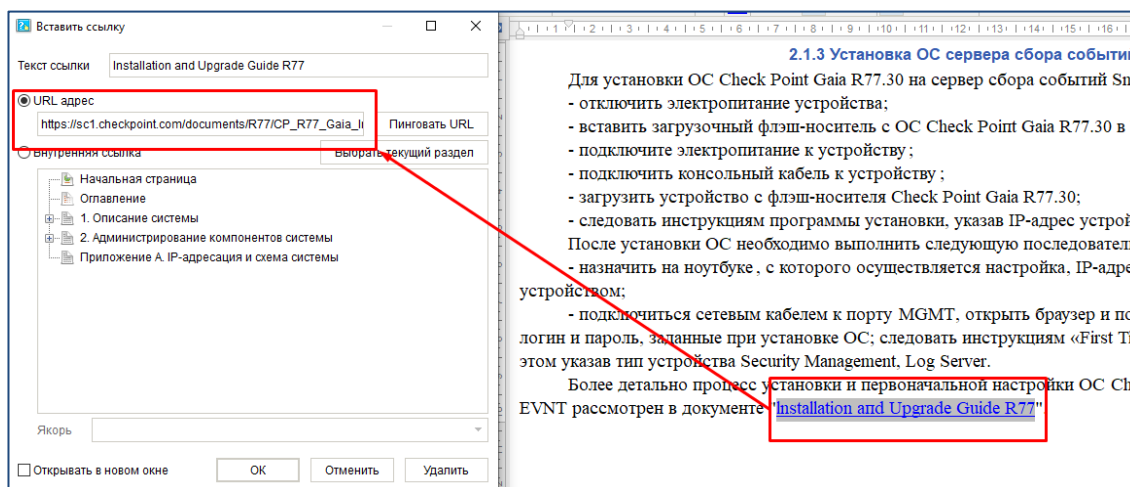


Рисунок 25 — Гиперссылки

После того, как руководство заполнено, были добавлены ключи, представленные на рисунке 26, они необходимы для более простого и конкретного поиска информации.

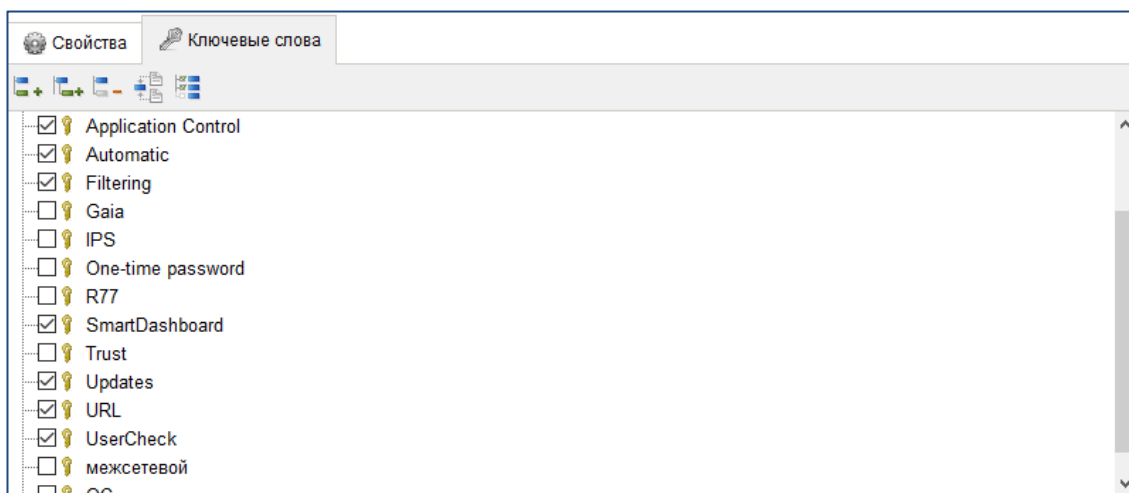


Рисунок 26 — Окно создания и настройки ключевых слов

Для того чтобы привязать ключ к какой-либо главе или подглаве, необходимо указать их в самом ключе, либо же в каждой главе выбрать нужный ключ, который подходит для данной главы. Так, например, для ключа с названием SmartDashboard было выбрано несколько глав, как показано на рисунке 27 в которых упоминается данное слово, а также непосредственно идет речь о настройке с помощью данного средства.

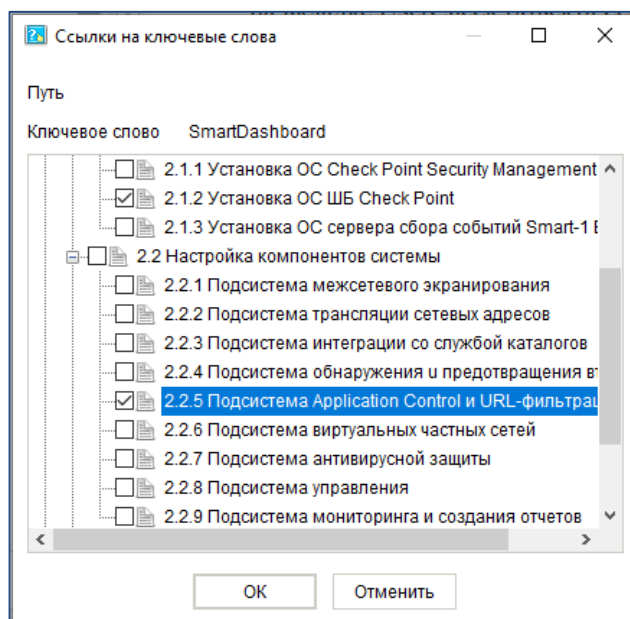


Рисунок 27 — Ссылки на ключевые слова

Для экспорта необходимо выбрать нужный формат, как на рисунке 28.

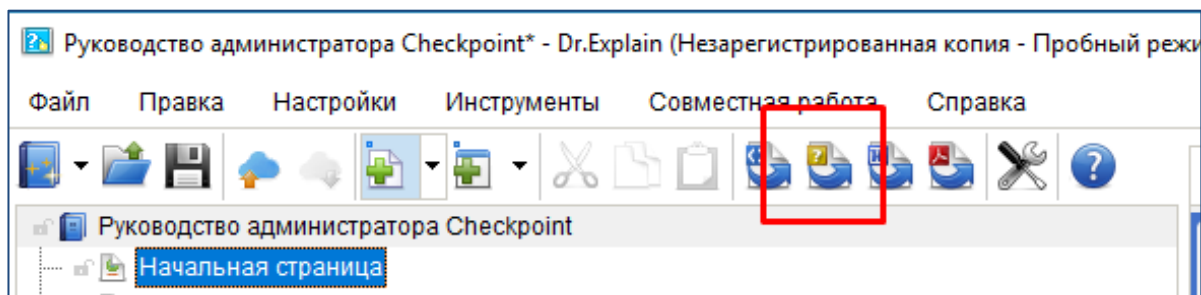


Рисунок 28 — Экспорт в выбранном формате

После выгрузки руководство было помещено в соответствующем месте, доступ к которому имеют лишь сотрудники, ответственные за администрирование комплекса Checkpoint.

Интерфейс руководства состоит из двух панелей, представлено на рисунке 29. Слева — панель навигации, справа — панель просмотра.

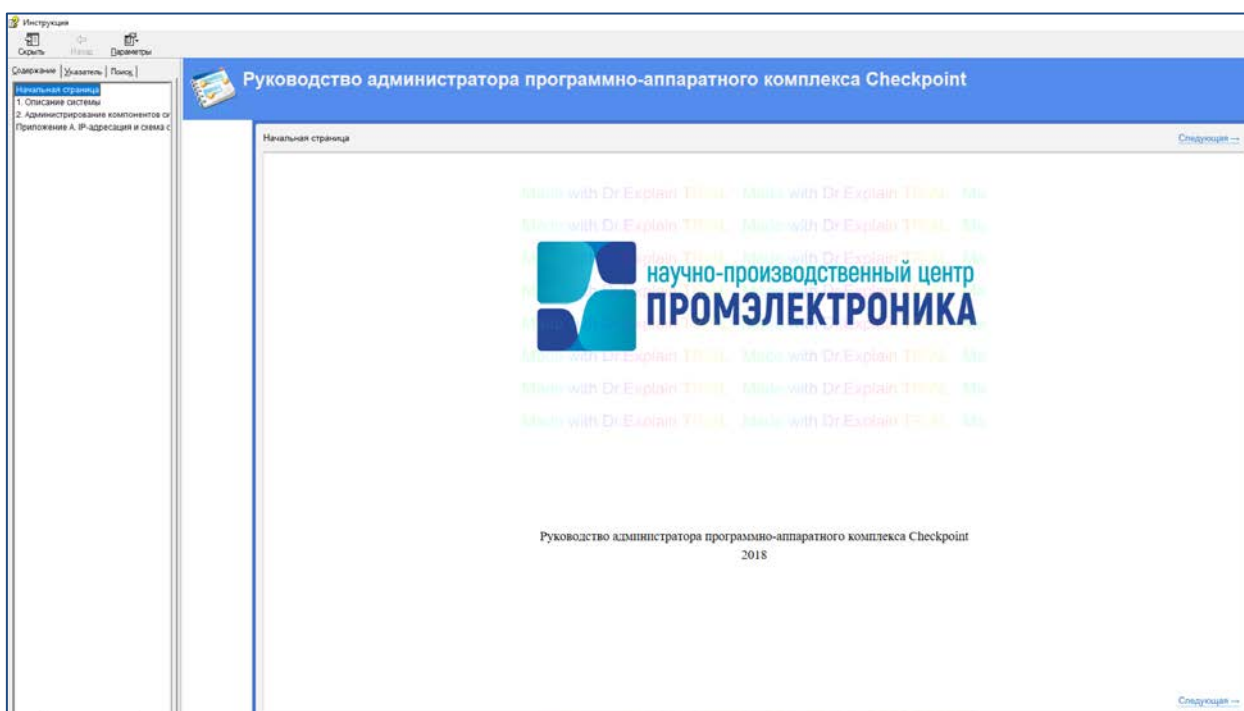


Рисунок 29 — Внешний вид

Но панель навигации разделена еще на 3 части. В нее входят: Содержание, Указатель, Поиск.

Во вкладке Меню, как изображено на рисунке 30, показано дерево разработанного руководства, составленное из разделов и подразделов.

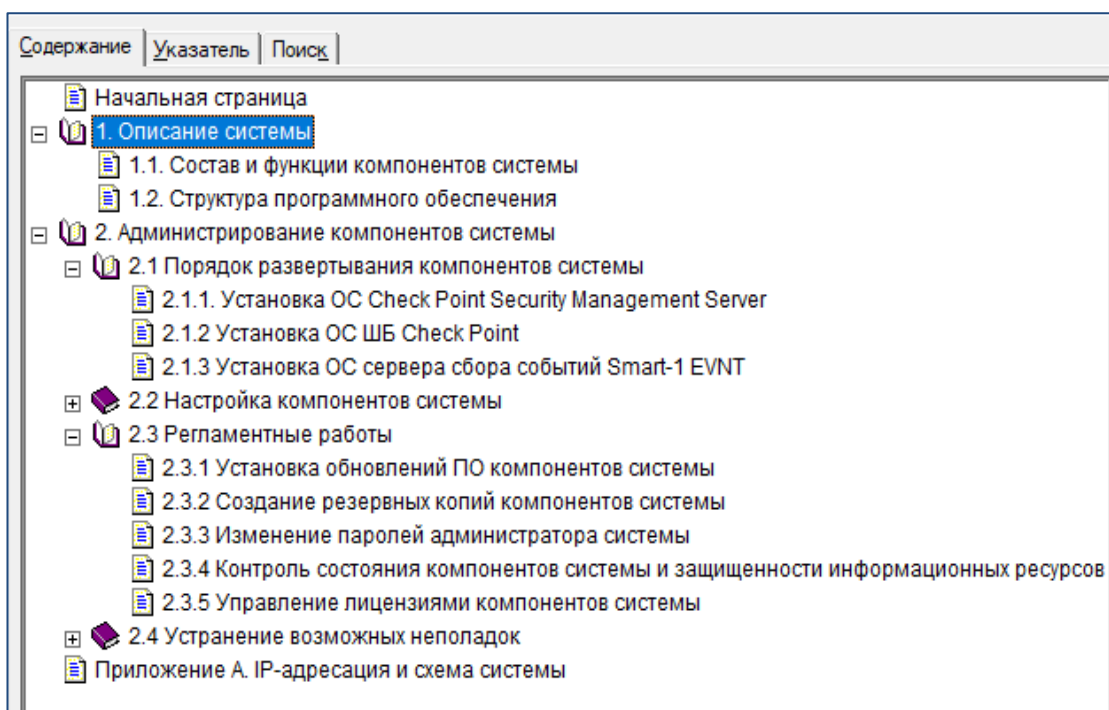


Рисунок 30 — Меню

Вкладка Указатель содержит все созданные ключи, а Поиск, представленный на рисунке 31, позволяет искать информацию по отдельным словам или фразам, что значительно улучшает поиск необходимой информации.

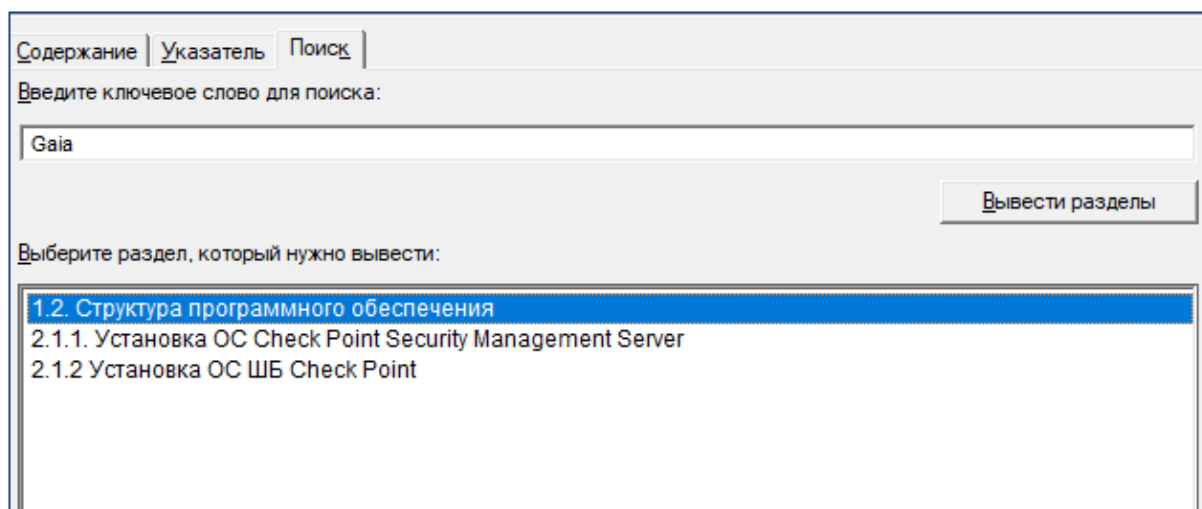


Рисунок 31 — Поиск

Разработанное руководство очень просто в использовании. В нем достаточно подробно расписан функционал и действия для выполнения основных задач необходимых для администрирования.

2.3 Содержание руководства администратора

В содержание руководства входят 2 основных раздела, это «Описание системы» и «Администрирование компонентов системы».

«Описание системы» включает в себя информацию о составе и функциях компонентов системы, места их установки, IP-адреса и вид установки (локально или в виде виртуальной машины). Это сделано для того, чтобы администратору, который обратится к данному руководству, было проще ориентироваться в схеме установки комплекса, что ускорит в дальнейшем выполнение поставленных задач, либо устранение неисправностей.

Вторым основным разделом является «Администрирование компонентов системы», он является основным, т.к. здесь объясняется, как устанавливать ОС Checkpoint на имеющиеся шлюзы безопасности, настраивать все подсистемы комплекса, проведение регламентных работ, а так же устранение неполадок. Он разделяется на 4 подраздела, в него входят: «Порядок развертывания компонентов», «Настройка компонентов системы», «Регламентные работы» и «Устранение возможных неисправностей».

В разделе «Порядок развертывания компонентов системы» объясняется как установить операционные системы на имеющиеся шлюзы безопасности, все расписано пошагово, чтобы у пользователя руководства не возникло вопросов в первоначальной настройке шлюзов, а так же приведена ссылка на официальную инструкцию, в случае, если все же появятся какие-то вопросы при установке, ссылка открывается в самом руководстве, как это выглядит представлено на рисунке 32 [21].

Раздел «Настройка компонентов системы» состоит из описания настройки всех блейдов программно-аппаратного комплекса Checkpoint для полной работоспособности в сети предприятия НПЦ «Промэлектроника», а также описание основных функций каждого компонента и интерфейса системы.

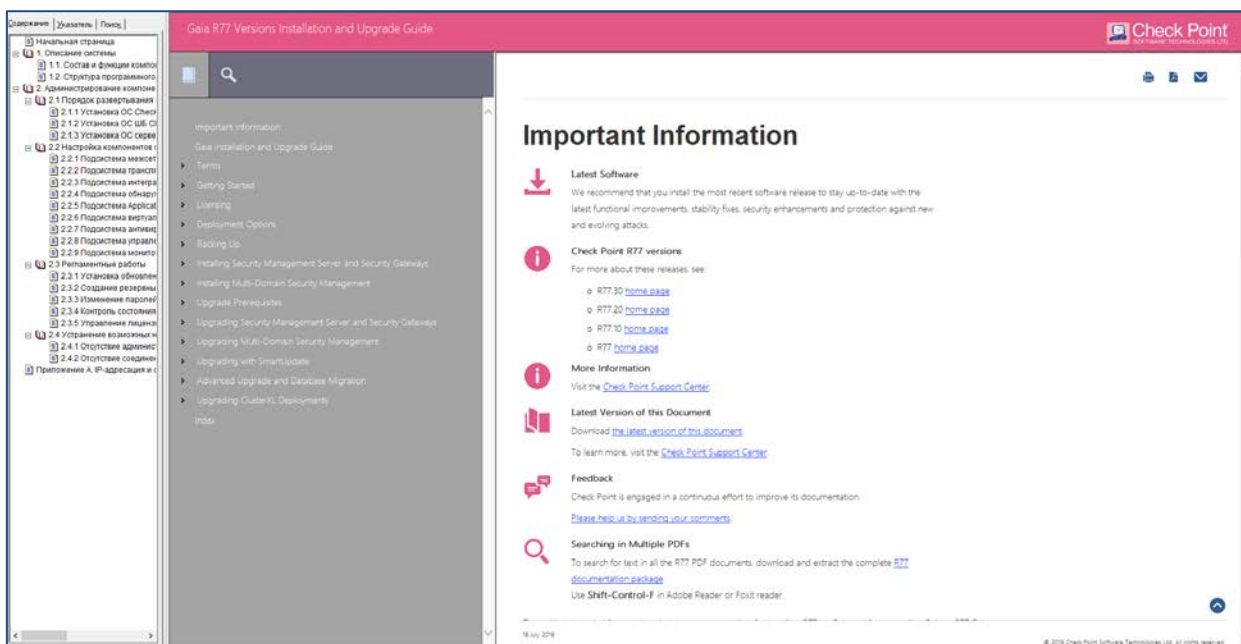


Рисунок 32 — Официальная инструкция

Например, в разделе «2.2.1 Подсистема межсетевое экранирования», рисунок 33, идет описание столбцов раздела Firewall.

Секция Rule Base содержит следующие основные столбцы:

- **NO** - номер правила политики безопасности;
- **HITS** - количество срабатываний;
- **NAME** - название правила политики безопасности;
- **SOURCE** - источник информации, подвергающейся проверке;
- **DESTINATION** - приемник информации, подвергающейся проверке;
- **VPN** - передача трафика с помощью VPN-соединения;
- **SERVICE** - сервис используемый при соединении;
- **ACTION** - действие, применяемое к данному пакету;
- **TRACK** - возможность регистрации и учета данных соединений;
- **INSTALL ON** - столбец, содержащий объекты, на которых применяется данное правило;
 - **TIME** - столбец, в котором определяются временные рамки действия правила;
- **COMMENTS** - комментарии к правилу.

Рисунок 33 — Описание столбцов раздела Firewall

В разделе посвященному трансляции сетевых адресов (Network Address Translation — NAT) расписано как создавать необходимые для данного функционала правила. Данный раздел необходим, т.к. регулярно появляются задачи на предоставление доступа в Интернет.

Интеграция со службой каталогов расписана очень подробно, т.к. является очень важным компонентом для полноценной работоспособности комплекса. При помощи данного блейда осуществляется идентификация пользователей, благодаря которому осуществляется или запрещается выход в Интернет конкретным категориям пользователей, в зависимости от их прав доступа.

«Подсистема обнаружения и предотвращения вторжений» так же является одной из важнейших систем комплекса, поэтому инструкция по ее настройке является обязательным для данного руководства.

Подсистема Application и URL-фильтрации дает возможность разрешать, блокировать или ограничивать доступ к миллионам Web-сайтов и приложений, и так как данный блейд активно используется на нашем предприятии, было решено добавить его в разрабатываемое руководство. Пример использования приведен на рисунке 34, на предприятии НПЦ «Промэлектроника» запрещено использование различных анонимайзеров [9].

No.	Hits	Name	Source	Destination	Applications/Sites	Action	Track
10	506K	block anomom traffic	Any	Internet	<ul style="list-style-type: none"> Private Internet ... Private Tunnel Browsec Anonine Anonymizer Anonymizer Uni... Anonymizers/pr... AnonymousIndex Anonymous Anonymox NetConceal Ano... Proxy based an... Steganos Intern... Proxy A4Proxy A5Proxy AliveProxy Betaproxy BypassProxyNow CGI-Proxy CProxy Camouflage Proxy Cgi-proxy.net Easy Proxy FlyProxy Freebieproxy.com Just Proxy Kproxy Kproxy Agent Megaproxy Ninjabproxy.com Nova Proxy Suite Online Proxy Ch... Paros proxy Proxy Rental Proxy4Free Proxy7 Telegram 	<ul style="list-style-type: none"> Block Blocked Message 	Log

Рисунок 34 — Запрещенные анонимайзеры

Следующим основным разделом является «Регламентные работы», в него включены инструкции по установке обновлений программного обеспечения компонентов системы, создание резервных копий, изменение паролей администратора, лицензирование и контроль за состоянием компонентов системы.

Добавление в руководство раздела «Резервное копирование» является обязательным, т.к. является неотъемлемой частью в работе любой информационной системы, его отсутствие может повлечь за собой необратимые последствия для предприятия. Оно обеспечивает быстрое восстановление системы в случае сбоя, поэтому в данном разделе были расписаны несколько вариантов создания бэкапов, через командную строку или графический интерфейс. Пример заполнения раздела изображен на рисунке 35, редактирование текста происходит аналогично программе Microsoft Word.

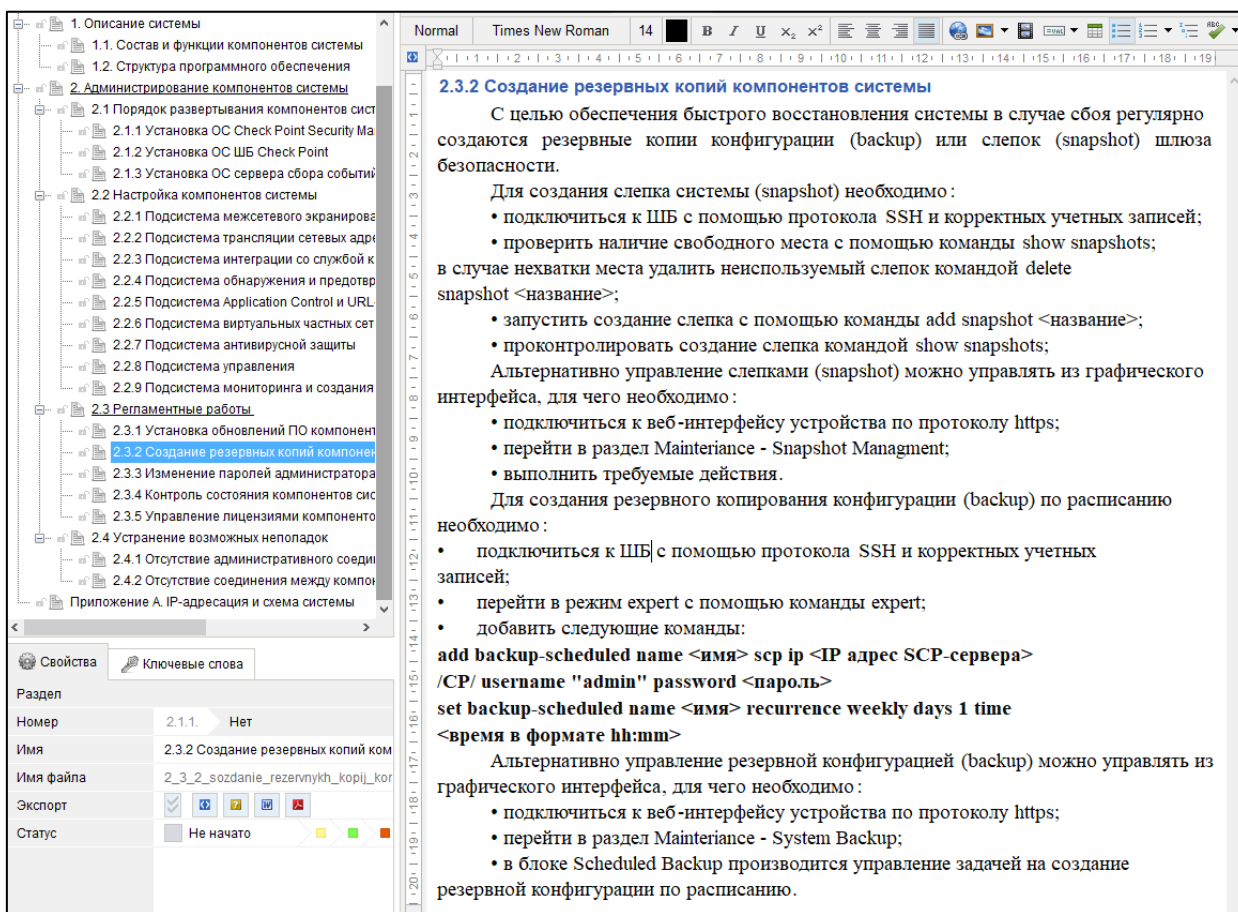


Рисунок 35 — Пример заполнения раздела

В разделе «Устранение возможных неполадок» на данный момент всего 2 раздела. В них описаны те проблемы, с которыми уже пришлось столкнуться в процессе эксплуатации программно-аппаратного комплекса Checkpoint. В дальнейшем его планируется дополнять по мере обнаружения различных нештатных ситуаций.

2.4 Методические рекомендации по использованию руководства

Для более эффективной организации использования разработанного руководства, необходимо разработать соответствующее методическое сопровождение, которое позволит повысить эффективность использования и обучения администратора функционалу программно-аппаратного комплекса Checkpoint.

Использование руководства в процессе ознакомления и обучения обеспечивает возможность:

- дать сотрудникам более полную, достоверную информацию об изучаемых функциях и процессах;
- повысить роль наглядности в образовательном процессе;
- удовлетворить запросы, желания и интересы сотрудников;
- освободить ответственного сотрудника от части технической работы, связанной с контролем и объяснения возможностей программно-аппаратного комплекса.

Так, для первоначального ознакомления с программно-аппаратным комплексом Checkpoint необходимо прочесть раздел «Описание» для того, чтобы понимать какое оборудование имеется в распоряжении и где оно установлено.

Далее, в порядке очередности изучить описание и инструкции по настройке всего функционала Checkpoint, одновременно подключившись к

консоли администратора в режиме просмотра, это позволит наглядно увидеть интерфейс программы для упрощения восприятия усваиваемой информации.

2.5 Апробация руководства администратора

Разработанное руководство администратора программно-аппаратного комплекса Checkpoint прошло апробацию в компании НПЦ «Промэлектроника».

На основании проведенной апробации было решено постоянно обновлять и дополнять разделы, т.к. со временем некоторая информация может стать неактуальной в связи с различными факторами, например, изменение сетевой инфраструктуры предприятия НПЦ «Промэлектроника», обновление версий операционной системы Checkpoint, а так же возникновение нестандартных ситуаций, чтобы их решение в дальнейшем занимало максимально короткое время.

ЗАКЛЮЧЕНИЕ

В настоящее время обеспечение информационной безопасности является важной проблемой, но ее решение видится во внедрении современных комплексов, однако такие системы, как правило, поставляются с документацией, выполненной на английском языке, что неудобно в виду не готовности современных инженеров в области англоязычной подготовки. Требуется разработка дополнительных методических средств на русском языке, таких как руководство администратора.

В рамках выпускной квалификационной работы было разработано руководство администратора программно-аппаратного комплекса Checkpoint, которое включает в себя описание и примеры выполнения всех стандартных задач во всех модулях.

На первом этапе выполнения выпускной квалификационной работы были проанализированы руководства пользователя, описывающие другие средства обеспечения информационной безопасности, и другие программные продукты. Далее была проанализирована литература и интернет-источники для определения функционального назначения и требований, предъявляемых к электронному руководству администратора.

На основании проведенного анализа были спроектированы структура и интерфейс руководства администратора, а также выбрано средство для его реализации — программный продукт для создания электронных справочных систем Dr.Explain.

На следующем этапе выполнения выпускной квалификационной работы было отобрано содержание руководства администратора, в который вошли следующие разделы: описание системы (состав комплекса), администрирование компонентов системы (установка и настройка), порядок развертывания компонентов системы (первоначальная установка и настройка), настройка компонентов системы (всех подсистем), регламентные рабо-

ты(обновление и резервное копирование), устранение возможных неполадок(отсутствие связи и т.п.), приложение (IP-адреса и схема системы).

Руководство пользователя прошло апробацию в компании НПЦ «Промэлектроника» которая показала, что использование данного руководства намного эффективнее, чем обучение по официальной документации программно-аппаратного комплекса Checkpoint, кроме того наличие четко обозначенной структуры и возможность быстрого перемещения внутри руководства также увеличивает скорость работы администратора и обращения к материалам руководства.

На заключительном этапе выполнения выпускной квалификационной работы были разработаны методические рекомендации по использованию разработанного руководства администратора, которые позволят повысить эффективность его использования на предприятии.

Таким образом, поставленные задачи можно считать выполненными, а цель достигнутой.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. «Аккорд» руководство по установке [Электронный ресурс]. — Режим доступа: http://www.accord.ru/docs/rau/install_rau.pdf (дата обращения: 12.12.2018).
2. Анализ программного обеспечения для создания электронного пособия [Электронный ресурс]. — Режим доступа: https://studwood.ru/1698115/informatika/analiz_programmnogo_obespecheniya_sozdaniya_elektronnogo_posobiya (дата обращения: 12.12.2018).
3. Инструкции и полезная документация Check Point [Электронный ресурс]. — Режим доступа: <https://habr.com/ru/company/tssolution/blog/344370/> (дата обращения: 12.12.2018).
4. Настройка Checkpoint. Часть 1. Установка и первоначальная конфигурация [Электронный ресурс]. — Режим доступа: <https://itnan.ru/post.php?c=1&p=259821> (дата обращения: 14.12.2018).
5. Научно-производственный центр «Промэлектроника» [Электронный ресурс]. — Режим доступа: <https://www.npcprom.ru/> (дата обращения: 12.12.2018).
6. Особенности разработки и структура руководства администратора для программного обеспечения [Электронный ресурс]. — Режим доступа: <https://articlekz.com/article/13265> (дата обращения: 12.12.2018).
7. Программа для создания книг и учебников SunRav BookOffice [Электронный ресурс]. — Режим доступа: <http://sunrav.ru/bookoffice.html> (дата обращения: 21.12.2018).
8. Программа для создания электронного руководства пользователя [Электронный ресурс]. — Режим доступа: <https://www.drexplain.ru/> (дата обращения: 22.12.2018).

9. Программный блейд URL Filtering [Электронный ресурс]. — Режим доступа: <https://www.checkpoint.com/ru/products/url-filtering-software-blade/> (дата обращения: 12.12.2018).

10. Руководство администратора по JaCarta SecurLogon [Электронный ресурс]. — Режим доступа: <https://www.aladdin-rd.ru/support/downloads/7d1f5844-2c54-404f-83ca-65c9e3e1193a/get> (дата обращения: 12.12.2018).

11. Создание help-файла (справки) в формате CHM для MS Access-приложения в Dr.Explain [Электронный ресурс]. — Режим доступа: https://www.drexplain.ru/articles/sozдание_fayla_spravki_v_formate_chm_dlya_ms_access_prilozheniya_v_dr_explain/ (дата обращения: 12.12.2018).

12. Удаленный доступ с мобильных устройств через VPN с помощью Check Point Mobile Access Blade [Электронный ресурс]. — Режим доступа: https://www.antimalware.ru/analytics/Technology_Analysis/VPN_Check_Point_Mobile_Access_Blade (дата обращения: 12.12.2018).

13. Шаблон «Руководство администратора» по ГОСТ 19 [Электронный ресурс]. — Режим доступа: <https://techwriters.ru/services/shablony/shablony-gost19/shablon-rukovodstvo-administratora-po-gost-19/> (дата обращения: 12.12.2018).

14. Application Control Software Blade [Электронный ресурс]. — Режим доступа: <https://www.checkpoint.com/products/application-control-software-blade/> (дата обращения: 12.01.2019).

15. Application Control и URL Filtering [Электронный ресурс]. — Режим доступа: https://rrc.ru/upload/checkpoint/Documentation-for-version-R75.40VS/CP_R75.40VS_ApplicationControlURLFiltering_AdminGuide_RUS.pdf (дата обращения: 05.01.2019).

16. Check Point AppWiki [Электронный ресурс]. — Режим доступа: <https://appwiki.checkpoint.com/appwikisdb/public.htm> (дата обращения: 12.12.2018).

17. Check Point. Что это, с чем его едят или коротко о главном [Электронный ресурс]. — Режим доступа <https://habr.com/ru/company/tssolution/blog/323606/> (дата обращения: 12.12.2018).

18. Checkpoint [Электронный ресурс]. — Режим доступа: https://ru.wikipedia.org/wiki/Check_Point (дата обращения: 12.12.2018).

19. Checkpoint Software Technologies ldt [Электронный ресурс]. — Режим доступа: <https://www.checkpoint.com/> (дата обращения: 22.01.2019).

20. Checkpoint на максимум. IPS. Часть 1 [Электронный ресурс]. — Режим доступа: <https://habr.com/ru/company/tssolution/blog/415083/> (дата обращения: 12.01.2019).

21. CheckPoint: установка, первоначальная настройка и организация кластера из двух фаервольных модулей [Электронный ресурс]. — Режим доступа: <https://habr.com/ru/company/muk/blog/200984/> (дата обращения: 12.12.2018).

22. Dr.Explain как инструмент технического писателя [Электронный ресурс]. — Режим доступа: <http://protext.su/pro/dr-explain-kak-instrument-tehnicheskogo-pisate/> (дата обращения: 22.01.2019).

23. HelpNDoc | HTML help authoring tool, Word, PDF and eBook documentation generator [Электронный ресурс]. — Режим доступа <https://www.helpndoc.com/> (дата обращения: 21.12.2018).

24. Managing Application Control and URL Filtering [Электронный ресурс]. — Режим доступа: https://sc1.checkpoint.com/documents/R76/CP_R76_AppControl_WebAdmin/60902.htm (дата обращения: 27.12.2018).

25. Mobile Access [Электронный ресурс]. — Режим доступа: https://rrc.ru/upload/checkpoint/Documentation-for-version-R75.40VS/CP_R75.40VS_MobileAccess_AdminGuide_RUS.pdf (дата обращения: 22.01.2019).

26. Mobile Access Software Blade [Электронный ресурс]. — Режим доступа: <https://www.checkpoint.com/products/mobile-access-software-blade/> (дата обращения: 22.01.2019).

27. Natata eBook Compiler 2.1 [Электронный ресурс]. — Режим доступа: <http://soft.sibnet.ru/soft/1756-natata-ebook-compiler-2-1/> (дата обращения: 12.12.2018).

28. Research Checkpoint [Электронный ресурс]. — Режим доступа: <https://research.checkpoint.com/> (дата обращения: 29.12.2018).

29. SunRav BookOffice [Электронный ресурс]. — Режим доступа: <https://www.sunrav.ru/bookoffice.html> (дата обращения: 12.12.2018).

30. TS Solution Системный интегратор [Электронный ресурс]. — Режим доступа: <https://tssolution.ru/> (дата обращения: 29.12.2018).

ПРИЛОЖЕНИЕ

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования

«Российский государственный профессионально-педагогический университет»

Институт инженерно-педагогического образования
Кафедра информационных систем и технологий
Направление подготовки 44.03.04 Профессиональное обучение (по отраслям)
Профиль «Информатика и вычислительная техника»
Профилизация «Информационная безопасность»

УТВЕРЖДАЮ
Заведующий кафедрой

И.А. Сулова

« ____ » _____ 2019 г.

ЗАДАНИЕ

на выполнение выпускной квалификационной работы бакалавра

студента (ки) _____ 4 _____ курса группы _____ *ЗИБ-401с*
_____ *Китанина Антона Владимировича*
_____ фамилия, имя, отчество полностью

1. Тема *Разработка руководства администратора программно-аппаратного комплекса checkpoint*

утверждена распоряжением по институту от « ____ » _____ 20 г. № ____

2. Руководитель _____ *Федулова Ксения Анатольевна*
_____ фамилия, имя, отчество полностью

_____ *доцент* _____ *к.пед.н.* _____ *доцент кафедры ИС* _____ *РГППУ*
ученая степень ученое звание должность место работы

3. Место преддипломной практики *АО «Промэлектроника-Инвест»*

4. Исходные данные к ВКР _____
Checkpoint на максимум. IPS. Часть 1 [Электронный ресурс]. — Режим доступа:
<https://habr.com/ru/company/tssolution/blog/415083/>

Инструкции и полезная документация Check Point [Электронный ресурс]. — Режим до-
ступа: <https://habr.com/ru/company/tssolution/blog/344370/>

Check Point. Что это, с чем его едят или коротко о главном [Электронный ресурс]. — Ре-

5. Содержание текстовой части ВКР (перечень подлежащих разработке вопросов)

Проанализировать литературу и интернет-источники для определения функционального назначения и требований, предъявляемых к электронному руководству администратора

Изучить необходимый функционал Checkpoint

Разработать электронное руководство администратора

6. Перечень демонстрационных материалов *презентация выполненная в MS Power Point, Разработанное руководство администратора*

7. Календарный план выполнения выпускной квалификационной работы

№ п/п	Наименование этапа дипломной работы	Срок выполнения этапа	Процент выполнения ВКР	Отметка руководителя о выполнении
1	Сбор информации по выпускной квалификационной работе	12.12.2018	10%	подпись
2	Выполнение работ по разрабатываемым вопросам и их изложение в пояснительной записке:		60%	подпись
2.1	Анализ проблем и тенденций	22.12.2018	10%	подпись
2.2	Анализ характеристик и специфических особенностей средств разработки продукта.	24.12.2018	10%	подпись
2.3	Разработка схемы и внешнего вида руководства	26.12.2018	10%	подпись
2.4	Разработка руководства администратора	28.12.2018	15%	подпись
2.5	Исправление недочетов руководства	30.12.2018	15%	подпись
3	Оформление текстовой части ВКР	03.01.2019	10%	подпись
4	Выполнение демонстрационных материалов к ВКР	07.01.2019	10%	подпись
5	Нормоконтроль	15.01.2019	5%	подпись
6	Подготовка доклада к защите в ГЭК	18.01.2019	5%	подпись

8. Консультанты по разделам выпускной квалификационной работы

Наименование раздела	Консультант	Задание выдал		Задание принял	
		подпись	дата	подпись	дата

Руководитель _____
подпись дата

Задание получил _____
подпись студента дата

9. Дипломная работа и все материалы проанализированы.

Считаю возможным допустить Китанина А.В. к защите выпускной квалификационной работы в государственной экзаменационной комиссии.

Руководитель _____
подпись дата

10. Допустить Китанина А.В. к защите выпускной квалификационной работы
фамилия и. о. студента

в государственной экзаменационной комиссии (протокол заседания кафедры от «__» _____ 20__ г., № _____)

Заведующий кафедрой _____
подпись дата