

РАЗРАБОТКА И РЕАЛИЗАЦИЯ МЕТОДА ЦЕНТРАЛИЗОВАННОЙ ПЕЧАТИ ДОКУМЕНТОВ

DEVELOPMENT AND IMPLEMENTATION OF A CENTRALIZED DOCUMENT PRINTING METHOD

**R. Dorokhin
S. Smirnov**

Summary. The paper considers a model of print management in departments with the development of restricted access documents. Developed a method for printing and labeling documents using additional modules written in the programming languages php and python. The result of this work is the development and justification of this method. In the course of this work was carried out the selection of optimal means of printing and labeling of restricted documents, designed a method for centralized document printing, as well as visualized the main components needed to implement the developed method.

Keywords: information security, information protection from unauthorized access, operating systems, mandated and discretionary access control.

Дорохин Руслан Андреевич
Аспирант, МГТУ им. Н.Э. Баумана
ruslandorohin00@gmail.com

Смирнов Сергей Николаевич
Доктор технических наук, МГТУ им. Н.Э. Баумана
smirnovsn@bmstu.ru

Аннотация. В работе рассмотрена модель управления печатью в подразделениях с разработкой документов ограниченного доступа. Разработан метод печати и маркировки документов с использованием дополнительных модулей, написанных на языках программирования php и python. Результатом данной работы является разработка и обоснование данного метода. В ходе данной работы был осуществлен выбор оптимальных средств печати и маркировки документов ограниченного доступа, спроектирован метод централизованной печати документов, а также визуализированы основные компоненты необходимые для осуществления разработанного метода.

Ключевые слова: информационная безопасность, защита информации от несанкционированного доступа, операционные системы, мандатное и дискреционное управление доступом.

Введение

В подразделениях с незначительным объемом документооборота и не имеющих машинописных бюро законодательство требует производить печать документов с грифом, только в подразделениях делопроизводства и режима (далее РСП) с использованием технических средств защиты информации. Станция печати секретных документов представляет собой объект вычислительной техники (далее ОВТ), состоящий из персонального компьютера. При необходимости печати документа сотрудник обязан зарегистрировать номера листов предварительного учета в соответствующем журнале в РСП, далее, если разработка производилась не на ОВТ расположенном в РСП, получить зарегистрированный съемный носитель информации и произвести на него запись. После чего сотрудник передает электронный носитель с документом в РСП для печати данного документа на твердую копию. Сотрудник РСП производит заполнение реквизитов документа в интерфейсе средств контроля печати, после чего производится печать документа. Данные о документе

автоматически регистрируются средствами защиты информации в электронном журнале маркировки отпечатанных документов. Данный алгоритм действий хоть и осуществляет контроль секретного документооборота, но в свою очередь имеет значительную угрозу утечки информации.

На основе данного исследования необходимо сформировать собственную методику построения системы контроля централизованной печати документов. Целями данного исследования являются:

1. Выбор оптимальных для методики средств защиты информации с реализованным функционалом централизованной печати документов.
2. Разбор основных особенностей системы печати выбранного продукта.
3. Спроектировать метод безопасной централизованной печати документов и визуализировать основные компоненты данного метода.
4. Реализовать разработанный метод путем настройки компонентов системы и разработке модулей.

```

cupsd.conf      interfaces      printers.conf  raw.types
cupsd.conf.pre16-bak  marker.template  printers.conf.0  snmp.conf
cups-files.conf  ppd            raw.convs      ssl

```

Рис. 1. Конфигурационные файлы сервера печати.

```

GNU nano 2.7.4      Файл: /etc/cups/marker.template
fonarik_border=5
charset=utf-8.PTAAstraSerif

last:normal:12:PTAAstraSerif:bottom-left:уч. {mac-inv-num}
last:normal:12:PTAAstraSerif:bottom-left:лист.№{CURRENT_PAGE}
last:normal:12:PTAAstraSerif:bottom-left:отп. {copies} экз.
last:normal:12:PTAAstraSerif:bottom-left:{mac-distribution}
last:normal:12:PTAAstraSerif:bottom-left:АС "ЭЛВС Управление №1"
last:normal:12:PTAAstraSerif:bottom-left:НЖМД уч.№{mac-workplace-id}
last:normal:12:PTAAstraSerif:bottom-left:исп. {JOB_OWNER}
last:normal:12:PTAAstraSerif:bottom-left:тел. {mac-owner-phone}
last:normal:12:PTAAstraSerif:bottom-left: {DATE}

any:bold:12:PTAAstraSerif:bottom-left:Войсковая часть 0000
any:normal:12:PTAAstraSerif:bottom-left:уч. {mac-inv-num}
any:normal:12:PTAAstraSerif:bottom-left:лист.№{CURRENT_PAGE}
any:normal:12:PTAAstraSerif:bottom-left: {DATE}

```

Рис. 2. Конфигурационный файл marker.template.

Средства защиты информации с реализованным функционалом централизованной печати документов

В данном разделе будут представлены наиболее популярные средства защиты информации от несанкционированного доступа (далее СЗИ от НСД) имеющиеся на Российском рынке.

Secret Net Studio — представляет собой наложенное СЗИ от НСД и используется в операционных системах (далее ОС) семейства Windows — [1]. Как указано в — [4] — управление печатью документов Secret Net Studio осуществляется в программе управления, имеющая возможность работы, как в локальном, так и в централизованном режиме. Также данное СЗИ от НСД имеет сертификат соответствия ФСТЭК России, который подтверждает соответствие требованиям руководящих документов по 3 классу защищенности СВТ, 2 классу защиты МЭ тип «В» (ИТ.МЭ.В2.ПЗ) — [7]. Что позволяет его использование в автоматизированных системах до классов 1Б, 2А, 3А включительно — [6]. Однако, согласно — [4], контроль за печатью документов осуществляет только Администратор безопасности и нет возможности предоставить доступ за контролем и управлением печатью сотруднику РСР.

Dallas Lock — как и первый продукт представляет собой наложенные СЗИ от НСД при использовании ОС Windows. А именно как указано в — [5] — СЗИ от НСД

Dallas Lock представляет собой программный комплекс системы защиты информации в ОС семейства Windows с возможностью подключения аппаратных идентификаторов. Подсистема позволяет правильно разграничить доступ к печати в соответствии с выбранной моделью разграничения доступа, а также к печатающим устройствам. Однако данный продукт имеет ограничения на использования в связи с постановлением правительства № 616 — применяющийся исключительно с ОС Windows.

ОС специального назначения «Astra Linux Special Edition» (далее ОС Astra Linux SE) представляет собой комплекс СЗИ от НСД на базе операционной системы семейства linux. Данная ОС не является наложенным средством и позиционирует себя как отечественная [9]. Также данная ОС имеет интернет ресурс с довольно обширной базой знаний. Однако, недолгое нахождение на рынке и малый опыт эксплуатации данной ОС сталкивают администраторов безопасности с рядом трудностей.

ОС Альт 8 СП для серверов и рабочих имеет в своём составе программные СЗИ от НСД и сертифицирована по требованиям безопасности информации, что подтверждают сертификаты соответствия ФСТЭК, МО РФ и ФСБ РФ. СЗИ от НСД ОС Альт 8 СП охватывают широкий спектр возможностей и функционала по защите информации — [8]. Однако данный Комплекс не имеет в своем составе средств маркировки документов, что не актуально для данного исследования.

Таблица 1. Описания параметров файла marker.template для оборота последней и для обратной стороны каждой страницы.

Наименование параметра	Описание параметра
Fonarik_border=5	Положение маркера на странице
charset=utf-8.PTAStraSerif	Кодировка документа и общий шрифт
Last:	Для параметров маркера, расположенного на последней странице
normal:	Тип шрифта
12: PT Astra Serif	Размер и наименование шрифта
bottom-left	Положение каждой строчки маркера
any	Для параметров маркера расположенного на всех страницах, кроме последней
{mac-inv-num}	Номер учетного листа документа
{CURRENT_PAGE}	Номер текущей страницы
{copies}	Номер экземпляра
{mac-distribution}	Список рассылки
{JOB_OWNER}	Имя отпечатавшего документ
{mac-owner-phone}	Номер телефона
{DATE}	Дата печати

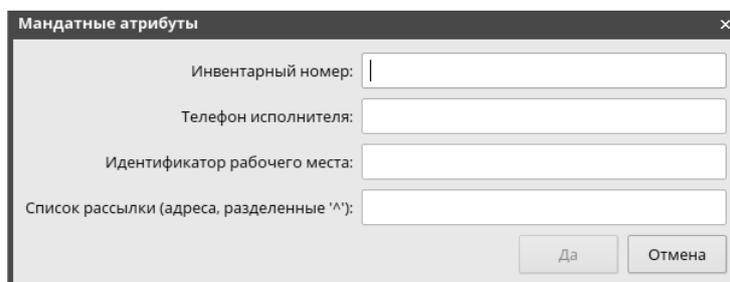


Рис. 3. Изменяемые параметры маркера при отправке документа на печать.

На основе данного анализа, для разработки метода централизованной печати была выбрана ОС Astra Linux SE. Данное решение связано по следующим причинам: 1) ОС является отечественным продуктом, что не противоречит постановлению правительства № 616; 2) функционал данной ОС позволяет гибко спроектировать и настроить систему централизованного управления печати; 3) разграничение доступа позволяет назначить необходимые привилегии сотрудникам РСП и дать им возможность вести аудит и настраивать печать исходя из особенностей каждого РСП.

Система печати и маркировки документов ОС Astra Linux SE

Система печати ОС Astra Linux SE основана на механизме CUPS, который позволяет управлять печатью документов, предоставлять информацию о распечатанных документах, состоянии принтеров, а также о пользователе, который производил печать. Конфигурационные файлы и каталоги cups расположены в каталоге «/etc/cups/», список которых представлен на рисунке 1.

В файле cupsd.conf содержатся параметры для функционирования сервера печати. Ниже представлены параметры маркера на обороте каждой страницы (рисунок 2), а также описание каждого маркера (таблица 1)

Проектирование метода централизованной печати документов на базе ОС Astra Linux SE

Из предыдущего раздела следует, что ОС Astra Linux обладает необходимым функционалом для реализации метода централизованной печати, однако в ходе эксплуатации данной ОС было выявлено ряд недостатков и трудностей в работе.

Первым и самым важным недостатком является отсутствие в руководстве в эксплуатации и интернет ресурсах инструкции по настройке и реализации сервера печати с использованием контроллера домена Free Ipa. Вторым недостатком является малый функционал настройки и печати маркеров при использовании

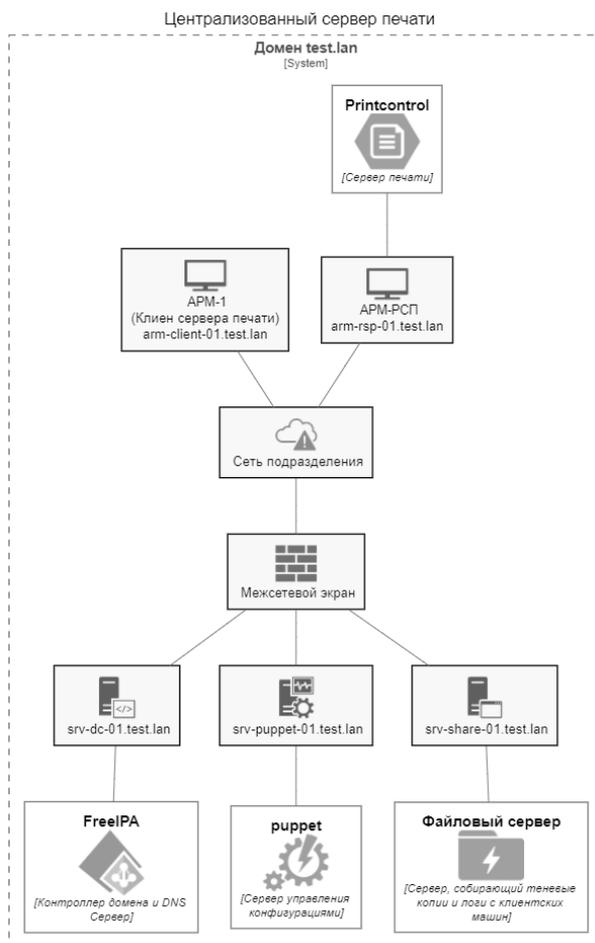


Рис. 4. Метод централизованной печати документов.

«flay-jobviewer», а именно: отсутствие возможности автоматически предоставлять данные из домена об учетном номере жесткого диска и телефоне исполнителя, малый набор и отсутствие возможности добавлять или удалять изменяемые параметры маркера при отправке на печать (рисунок 3).

Исходя из руководящих документов по защите информации и документов по обеспечению режима секретности, разработан следующий процесс печати:

1. Пользователь, разработав документ в сессии отличной от нуля, отправляет его на печать.
2. Печать документа не происходит, происходит отправка на сервер печати, находящийся в РСР подразделения.
3. Пользователь оповещает РСР об отправленном документе.
4. Сотрудник РСР регистрирует документ и предоставляет необходимые атрибуты для маркировки.
5. Сотрудник РСР отправляет документ на печать. После чего производится печать документа.

6. Данные о печати документа автоматически регистрируются в электронном журнале, а теневые копии отправляются на файловый сервер подразделения по защите информации.

На рисунке 4 представлена схема реализации метода централизованной печати документов.

В следующем разделе будет представлена настройка сервера печати для работы в едином пространстве пользователей в домене FreeIPA согласно инструкции представленной технической поддержкой Astra Linux.

Настройка сервера печати для работы в домене FreeIPA

Общий состав стенда представлен в табл. 2.

На первом этапе необходимо настроить контроллер домена для этого выполнить следующие действия:

1. Создать в web интерфейсе или с помощью командной строки на сервере доменную группу

Таблица 2. Состав стенда для реализации централизованной печати документов

Доменное имя	Ip адрес/маска сети	Назначение
srv-dc-01.test.lan	192.168.1.2/29	Контроллер домена FreeIpa
srv-puppet-01.test.lan	192.168.1.3/29	Сервер управления конфигурациями puppet
srv-share-01.test.lan	192.168.1.4/29	Файловый сервер для централизованного сбора и хранения теневых копий и журналов печати и маркировки документов
«Рубикон»	192.168.1.1/29 192.168.2.1/30	Межсетевой экран. Представлен для полной реализации метода централизованной печати документов. В рамках данной работы не применяется.
arm-rsp-01.test.lan	192.168.2.2/30	Сервер печати документов
arm-client-01.test.lan	192.168.2.3/30	Клиент сервера печати под управлением контроллера домена freeIpa

```

administrator@arm-rsp-01:~$ sudo ktutil
ktutil: rkt /tmp/ipp.keytab
ktutil: wkt /etc/krb5.keytab
ktutil: l
slot KVNO Principal
-----
1 1 ipp/arm-rsp-01.test.lan@TEST.LAN
2 1 ipp/arm-rsp-01.test.lan@TEST.LAN
ktutil: q
administrator@arm-rsp-01:~$ sudo klist -kte /etc/krb5.keytab
Keytab name: FILE:/etc/krb5.keytab
KVNO Timestamp Principal
-----
1 18.05.2020 12:10:17 host/arm-rsp-01.test.lan@TEST.LAN (aes256-cts-hmac-sha1-96)
1 18.05.2020 12:10:17 host/arm-rsp-01.test.lan@TEST.LAN (aes128-cts-hmac-sha1-96)
1 18.05.2020 13:10:27 ipp/arm-rsp-01.test.lan@TEST.LAN (aes256-cts-hmac-sha1-96)
1 18.05.2020 13:10:27 ipp/arm-rsp-01.test.lan@TEST.LAN (aes128-cts-hmac-sha1-96)
    
```

Рис. 5. Добавление ключей в хранилище Kerberos.

```

sudo cupsctl --remote-admin --share-printers --remote-any
sudo cupsctl ServerAlias=*
sudo cupsctl DefaultPolicy=authenticated
sudo cupsctl MarkerUser=ipp
sudo cupsctl ServerName=arm-rsp-01.test.lan
sudo cupsctl MacEnable=on
sudo cupsctl DefaultAuthType=Negotiate
    
```

Рис. 6. Изменение настроек сервера печати.

- и пользователя, добавить созданного пользователя в созданную группу.
- Добавить созданного пользователя в локальную группу lpmac на сервере печати: «sudo gpasswd -a gc_print_admin lpmac»
- На контроллере домена FreeIpa создать службу ipp командой: «ipa service-add ipp/arm-rsp-01.test.lan»
- Выгрузить таблицу ключей для службы ipp/arm-rsp-01.test.lan @TEST.LAN: «sudo ipa-getkeytab -p ipp/arm-rsp-01.test.lan@TEST.LAN -k /tmp/ipp.keytab»

- Перенести таблицу ключей на сервер печати: «scp /tmp/ipp.keytab administrator@arm-rsp-01.test.lan:/tmp»

Следующим этапом необходимо произвести настройку сервера печати:

- Добавить созданные ключи в хранилище Kerberos как показано на рисунке 5:
- Изменить группу администратора печати на созданную доменную группу, для этого изменить значение в файле /etc/cups/cups-files.conf с SystemGroup lpadmin на SystemGroup print_admins

```

<!DOCTYPE HTML>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>Сервер печати</title>
<!--Подключение стилей bootstrap-->
<link rel="stylesheet"
href="/printcontrol/prog/css/bootstrap-4.5.0-dist/css/bootstrap.min.css">
</head>
<!--Добавление изображения в качестве фона -->
<body style="background-image: url('/printcontrol/prog/css/printer.jpg');
background-size: 100%; opacity:0.7;">
<div class="container">
<div class="row">
<div style="margin-left:auto;
margin-right:auto;margin-top:200px;">
<!--Ссылка на приложение printcontrol-web-->
<form action="/printcontrol/prog/printcontrol.php">
<button type="submit" class="template-2">
Начать работу с сервером печати!
</button>
</form>
</div>
</div>
</div>
<!--Подклчение библиотеки для работы скриптов bootstap4 -->
<script src="/printcontrol/prog/css/jquery-3.5.1.js"></script>
<!--Подключение собственной страницы с java script-->
<script src="/printcontrol/prog/css/main.js"></script>
<!--Подключение java script bootstrap4-->
<script
src="/printcontrol/prog/css/bootstrap-4.5.0-dist/js/bootstrap.min.js">
</script>
</body>
</html>

```

Код 1

```

<form method="post" action="template.php">
<button type="submit">
Редактировать маркер
</button>
</form>

```

Код 2

```

<div class="container">
<div class="row">
<!-- Кнопки для вызова модального окна-->
<div style="margin-left:auto; margin-right:auto;margin-top:200px;">
<button type="submit" id="1" data-toggle="modal" data-target="#exampleModal" class="template1">
Маркер для всех и последней страницы
</button>
<button type="submit" id="2" data-toggle="modal" data-target="#exampleModal" class="template-1">
Маркер для последней страницы
</button>
<button type="submit" id="3" data-toggle="modal" data-target="#exampleModal" class="template-1">
Маркер для любой страницы
</button>
</div>
</div>
<div class="row">
<a href="/printcontrol/prog/printcontrol.php"
class="btn btn-lg btn-secondary btn-block"
style="margin-top:10px; margin-left:auto; margin-right:auto; width: 640px;">
Вернуться на сервер печати
</a>
</div>
</div>
</div>
</div>
<!-- Модальное окно для редактирования параметров маркера -->
<div class="modal fade" id="exampleModal" tabindex="-1" role="dialog" aria-
labelledby="exampleModalLabel" aria-hidden="true" >
<div class="modal-dialog">
<div class="modal-content" style="width: 600px;">
<div class="modal-header">
<h5 class="modal-title" id="exampleModalLabel">Редактор маркера</h5>
<button type="button" class="close" data-dismiss="modal" aria-label="Close">
<span aria-hidden="true">&times;</span>
</button>
</div>
<div class="modal-body" >
<!--Отправка формы на страницу с функцией изменения параметров маркера-->
<form method='post' action='/printcontrol/prog/function.php'>
<textarea name='marker' id="text" class="form-control" rows="17">
fonarik_border=5
charset=utf-8.ПТАstraSerif
last:normal:12:PT Astra Serif:bottom-left:уч. {mac-inv-num}с
last:normal:12:PT Astra Serif:bottom-left:лист. № {CURRENT_PAGE}
last:normal:12:PT Astra Serif:bottom-left:отп. {copies} экз.
last:normal:12:PT Astra Serif:bottom-left: {mac-distribution}
last:normal:12:PT Astra Serif:bottom-left:АС "Управление №1"
last:normal:12:PT Astra Serif:bottom-left:НЖМД уч.№ {mac-workplace-id}
last:normal:12:PT Astra Serif:bottom-left:исп. {JOB_OWNER}
last:normal:12:PT Astra Serif:bottom-left:тел. {mac-owner-phone}
last:normal:12:PT Astra Serif:bottom-left: {DATE}
any:bold:12:PT Astra Serif:bottom-left:Войсковая часть 0000

```

Код 3 (продолжение на стр. 83)

```

any:normal:12:PT Astra Serif:bottom-left:уч №{mac-inv-num}c
any:normal:12:PT Astra Serif:bottom-left:лист №{CURRENT_PAGE}
any:normal:12:PT Astra Serif:bottom-left:{DATE}
</textarea>
</div>
<div class="modal-footer">
<button type="button" class="btn btn-secondary" data-dismiss="modal">Закрыть</button>
<button type="submit" class="btn btn-danger">Сформировать маркер</button>
</form>
</div>
</div>
</div>
</div>
</div>
</div>
<script src="/printcontrol/prog/css/jquery-3.5.1.js"></script>
<script src="/printcontrol/prog/css/main.js"></script>
<script src="/printcontrol/prog/css/bootstrap-4.5.0-dist/js/bootstrap.min.js"></script>
<script>
//Функция для кнопки редактирования маркера для всех страниц
$('#2').click(function () {
$('#text').html('fonarik_border=5\ncharset=utf-8.PTAstraSerif\n\nany:normal:12:PT Astra Serif:bottom-
left:уч. {mac-inv-num}c\nany:normal:12:PT Astra Serif:bottom-left:лист. №
{CURRENT_PAGE}\nany:normal:12:PT Astra Serif:bottom-left:отп. {copies} экз.\nany:normal:12:PT
Astra Serif:bottom-left:{mac-distribution}\nany:normal:12:PT Astra Serif:bottom-left:АС "Сегмент ЗЛВС
ЦЗИ от ТР"\nany:normal:12:PT Astra Serif:bottom-left:НЖМД уч.№ {mac-workplace-
id}\nany:normal:12:PT Astra Serif:bottom-left:исп. {JOB_OWNER}\nany:normal:12:PT Astra
Serif:bottom-left:тел. {mac-owner-phone}\nany:normal:12:PT Astra Serif:bottom-left:{DATE}');
});
//Функция для кнопки редактирования маркера для последней страницы
$('#3').click(function () {
$('#text').html('fonarik_border=5\ncharset=utf-8.PTAstraSerif\n\nany:bold:12:PT Astra Serif:bottom-
left:Войсковая часть 3061\nany:normal:12:PT Astra Serif:bottom-left:уч №{mac-inv-
num}c\nany:normal:12:PT Astra Serif:bottom-left:лист №{CURRENT_PAGE}\nany:normal:12:PT Astra
Serif:bottom-left:{DATE}');
});
</script>

```

Код 3 (продолжение)

3. Далее необходимо внести изменения в конфигурационный файл /etc/cups/cupsd.conf, для этого лучше воспользоваться утилитой cupsctl (рисунок 6):
4. В конфигурационном файле /etc/cups/cupsd.conf с помощью текстового редактора необходимо заменить строки Port 631 и Listen /var/run/cups/cups.sock на Listen 0.0.0.0:631
5. Открыть fly-admin-printer и в настройках принтера указать политику parsec, а также необходимые уровни конфиденциальности для печати под ненулевым уровнем.

Последним этапом настройки сервера печати для работы в домене FreeIPA является настройка клиентских машин.

Разработка дополнительных функций для менеджера печати

Как упоминалось в предыдущих разделах, в качестве оболочки для работы с отправленными на печать документами была выбрана утилита «printcontrol-web». В качестве стилизации страниц был использован фреймворк bootstrap4. Для доступа к базе LDAP необходимо установить библиотеку php7.0-ldap

На первом этапе необходимо создать стартовую страницу с ссылкой на файл printcontrol.php для удобного перехода на страницу управления печатью (код 1).



Рис. 7. Кнопки для вызова модального окна с параметрами маркера

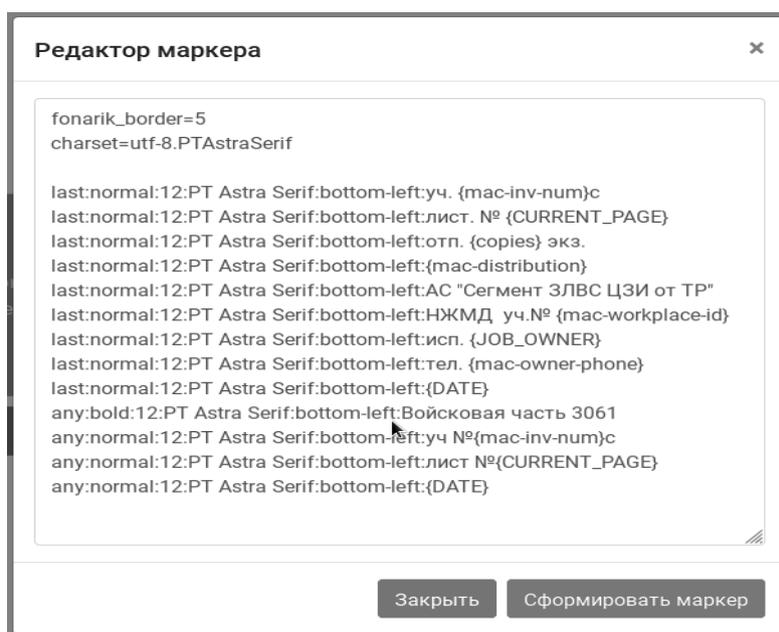


Рис. 8. Модальное окно для редактирования всех страниц

Следующим шагом необходимо предоставить возможность администратору печати изменять параметры маркера находясь в веб приложении. Для этого необходимо добавить кнопку с переходом на страницу редактирования маркеров в тег xml файла printcontrol.xml (код 2).

В файле template.php находятся шаблоны для маркеров и кнопки вызывающие модальные окна для редактирования параметров маркера (рисунок 7 и 8, код 3).

На странице function.php находится функция, которая добавляет отправленные данные в файл /etc/cups/marker.template (код 4).

Следующим этапом является получение данных из базы LDAP. Следует заметить, что атрибута для жесткого дика нет, поэтому был использован атрибут

«userclass». Данный атрибут принадлежит группе информации о хосте. Для реализации данного функционала необходимо добавить фрагмент программного кода в файл printcontrol.php (код 5).

Реализация централизованного аудита печати и маркировки документов

Следующим шагом необходимо обеспечить со всех РСЦ централизованный сбор журналов печати и маркировки документов, а также теневого копий. Монтирование сетевой шары приемлемо осуществить с помощью сервера конфигурации puppet и небольшого скрипта на языке программирования python.

Содержимое манифеста puppet представлено в коде 6:

```

<?php
//Установка кодировок
setlocale(LC_CTYPE,'ru_RU.cp1251');
setlocale(LC_COLLATE,'ru_RU.cp1251');
setlocale(LC_ALL,'ru_RU.UTF-8');
//Изменение файла marker.template
system('echo `escapeshellarg($_POST[marker]).`> /etc/cups/marker.template');
//Редирект на страницу template.php
header("location:http://arm-rsp-01.test.lan/printcontrol/prog/template.php");
?>

```

Код 4

```

putenv("KRB5CCNAME={$_SERVER['KRB5CCNAME']}");
//Получение полного имени администратора печати
$admin_info=posix_getpwuid(posix_geteuid());
$print_admin = $admin_info['gecos'];
.....
$time_at_creation["date"] = date("d.m.Y", $p["time-at-creation"]);
$time_at_creation["time"] = date("H:i:s", $p["time-at-creation"]);
//Получение и добавление в шаблон полного имени пользователя
//отправившего документ на печать
$user_name = $Job->addChild("user-name"); //Получение тега с именем из xml
$user2 = $u[0];
$user_info=posix_getpwnam($user2);
$user_name["name"]=$user_info['gecos']; //Полное имя пользователя
//Подключение к серверу LDAP
$ldapconn=ldap_connect('srv-dc-01.test.lan', 389)
or die ("Некорректен");
ldap_set_option($ldapconn, LDAP_OPT_PROTOCOL_VERSION, 3);
ldap_set_option($ldapconn, LDAP_OPT_REFERRALS, 0);
$ldapbind=ldap_sasl_bind($ldapconn, NULL, NULL, 'GSSAPI', 'TEST.LAN', "", "") or die('Ошибка
подключения'); //Подключение к LDAP с использованием Kerberos
//Получение номера телефона пользователя
$user_phone = $Job->addChild("user-phone"); //Получение тега «Номер телефона» из xml
$us = $u[0];
$uid="uid=".$us;
//Параметры поиска по дереву LDAP
$result=ldap_search($ldapconn,"dc=test, dc=lan",$uid)
or die ("Некорректен");
$info=ldap_get_entries($ldapconn, $result);
$user_phone["name"]=$info[1][telephonenumber][0];
//Получение номера жесткого диска с хоста, откуда была отправлена печать
$host = $Job->addChild("host");
$hostjob=exec('lptr -j '.$p["job-id"].' -q job-originating-host-name'); //Получаем ip адрес хоста
$hoststring=substr($hostjob,26); //обрезаем строку и получаем чистый ip адрес
$hos=gethostbyaddr($hoststring); //Узнаем имя хоста при существующей зоне обратного просмотра
$uid="cn=".$hos; Название контейнера хоста
$result=ldap_search($ldapconn,"dc=test, dc=lan",$uid)
or die ("Некорректен"); //Поиск по дереву базы LDAP
$info=ldap_get_entries($ldapconn, $result);
$host["name"]=$info[0][userclass][0]; //добавляем номер жесткого диска в шаблон

```

Код 5

```

#Создание файла с паролем для доступа к административному ресурсу
file {'/root/user.txt':
  ensure => 'present',
  replace => 'no',
  content => "username=administrator\npassword=Gthbvtnh2019\n",
  mode => '0644',
}
#Перенос скрипта для изменения настроек fstab
file {'/tmp/fstab.py':
  ensure => 'file',
  mode => '744',
  owner => 0,
  source => 'http://srv-repo-01/config/fstab.py',
}
#Запуск скрипта
exec {'generate the conf':
  command => '/tmp/fstab.py',
  cwd => '/tmp/',
  user => 'root',
}

```

Код 6

```

#!/usr/bin/python3.5
import subprocess
import socket

host = socket.gethostname() # Получение имени сервера печати
word = "//srv-shadow-cups-01.secret.eip/shadow_copies/" + host + "/var/spool/cups/parsec/ cifs
rw,auto,credentials=/root/user.txt,rw,noperm 0 0\n"
inp = iter(open('/etc/fstab').readlines()) # Чтение содержимого файла fstab
#Проверка всех строк на отсутствие строки с административным ресурсом
for i in inp:
  if word in i:
    a = 0
  else:
    a = 1
  if a == 1:
    #Добавление строки при отсутствии в файле
    with open('/etc/fstab', 'a') as file:
      file.write(word)
      file.close()
    subprocess.run(["mount", "-a"])#Выполнение монтирования

```

Код 7

После применения конфигурации puppet, на серверах печати запустится скрипт, который произведёт монтирование директории с именем сервера печати в «/var/spool/cups/parsec». Содержимое скрипта fstab.py представлено в коде 7.

Заключение

Таким образом, данное исследование установило, что наиболее приемлемым средством защиты для гибкого проектирования системы защищенной печати

документов в подразделении является ОС Astra linux SE. Данная ОС позволит разработать дополнительные модули и вести строгий аудит за отпечатанными документами. Механизм системы печати ОС Astra linux SE реализован на основе службы «CUPS», который используется в большинстве дистрибутивов linux и позволяет получать подробную информацию о процессе печати и об участвующих в нем субъектах (пользователях).

Спроектированный в данной статье метод позволит вести строгий контроль печати документов. Данный метод позволяет задерживать документы отправленные, на печать и направлять их администратору печати, хранить все данные о пользователе в доменной базе сервера LDAP и получать необходимую информацию автоматически. Это решение достигнуто благодаря ис-

пользованию библиотеки «php7.0-ldap», которая позволяет производить подключение к серверу LDAP (в рамках данной статьи — это FreeIPA) и получать информацию о всех разрешенных объектах базы. Дополнительно был разработан функционал редактирования маркеров документа в приложении printcontrol-web. Сбор всех журналов маркировки, путем монтирования административного сетевого ресурса, позволит администраторам безопасности вести аудит за каждым отпечатанным документом без необходимости опрашивать сервера печати по отдельности. Это решение было реализовано с помощью сервера управления конфигурациями «puppet» и скриптов на языке программирования python. Журналы печати и маркировки, а также теньевые копии хранятся в каталоге /var/spool/cups/, именно в этот каталог и было произведено монтирование сетевого ресурса.

ЛИТЕРАТУРА

1. Кирпичников М.Р. Механизмы защиты КСЗИ на примере Secret Net Studio // Молодежная научная школа кафедры «Защищенные системы связи». 2020. Т. 1. № 1 (1). С. 35–38.
2. Операционная система специального назначения «ASTRA LINUX SPECIAL EDITION» Руководство администратора. Часть 1. 2018. — 319 с.
3. Операционная система специального назначения «ASTRA LINUX SPECIAL EDITION» Руководство по КСЗ. Часть 1. РУСБ. 2018. — 172 с.
4. Средство защиты информации Secret Net Studio — С. Руководство администратор. Настройка и эксплуатация. Локальная защита. RU.88338853.501400.002 91 5, 2019. — 159 с.
5. Руководство по эксплуатации КЗИ НСД Dallas Lock 8.0 RU.48957919.501410–02 92, 2017. — 356 с.
6. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.
7. <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00> Реестр КЗИ ФСТЭК России.
8. Некрасова, Е. Российская операционная система для критической информационной инфраструктуры: новая версия ОС «Альт 8 СП» [Текст] / Е. Некрасова // БИТ. Бизнес & Информационные технологии. / Издательский дом «Положевец и партнеры». — Москва, 2021. — Вып. 1(104). — С. 40–42.
9. Дорохин Р.А. Анализ особенностей системы защиты операционной системы Astra Linux 1.6 SE / Дорохин Р.А., Безродных О.А., Смирнов С.Н., Майстренко В.А. // Динамика сложных систем — XXI век. 2021. Т. 15. № 1. С. 38–47.
10. <https://wiki.astralinux.ru>