ТОЧНАЯ НАУКА

естественнонаучный журнал

XLIII Международная научная конференция
"Техноконгресс"

Сборник статей международной естественнонаучной конференции с публикацией в НЭБ elibrary.ru

t-nauka.ru

КЕМЕРОВО 2019

СБОРНИК СТАТЕЙ СОРОК ВТОРОЙ МЕЖДУНАРОДНОЙ НАУЧНОЙ КОНФЕРЕНЦИИ «ТЕХНОКОНГРЕСС»

17 июня 2019 г.

ББК Ч 214(2Рос-4Ке)73я431

ISBN 978-5-9907998-1-3

Кемерово УДК 378.001. Сборник статей студентов, аспирантов и профессорско-преподавательского состава. По результатам XLIII Международной научной конференции «Техноконгресс», 17 июня 2019 г. www.t-nauka.ru / Редкол.:

Никитин Павел Игоревич - главный редактор, ответственный за выпуск журнала

Баянов Игорь Вадимович - математик, специалист по построению информационно-аналитических систем, ответственный за первичную модерацию, редактирование и рецензирование статей

Артемасов Валерий Валерьевич - кандидат технических наук, ответственный за финальную модерацию и рецензирование статей

Зимина Мария Игоревна - кандидат технических наук, ответственный за финальную модерацию и рецензирование статей

Нормирзаев Абдукаюм Рахимбердиеви - кандидат технических наук, Наманганский инжинерно-строительный институт (НамМПИ)

Безуглов Александр Михайлович - доктор технических наук, профессор кафедры математики и математического моделирования, Южно-российский государственный политехнический университет (Новочеркасский политехнический институт) им. М.И .Платова,

Наджарян Микаел Товмасович - кандидат технических наук, доцент, Национальный политехнический университет Армении

Шушлебин Игорь Михайлович - кандидат физико-математических наук, кафедра физики твёрдого тела Воронежского государственного технического университета

Равшанов Дилшод Чоршанбиевич - кандидат технических наук, заведующий кафедрой «Технология, машины и оборудования полиграфического производства», Таджикский технический университет имени академика М.С.Осими

Крутякова Маргарита Викторовна – доцент, кандидат технических наук, Московский политехнический университет

Гладков Роман Викторович - кандидат технических наук, доцент кафедры эксплуатации вооружения и военной техники Рязанского гвардейского высшего воздушно-десантного командного училища

Моногаров Сергей Иванович - кандидат технических наук доцент Армавирского механико-технологического института (филиал) ФГОУ ВО КубГТУ

Шевченко Сергей Николаевич - кандидат технических наук, доцент кафедры СЭУ, Балтийская государственная академия рыбопромыслового флота РФ

Отакулов Салим - Доктор физико-математических наук, профессор кафедры высшей математики Джизакского политехнического института

А.О. Сергеева (ответственный администратор)[и др.];

Кемерово 2019

В сборнике представлены материалы докладов по результатам научной конференции.

Цель – привлечение студентов к научной деятельности, формирование навыков выполнения научно-исследовательских работ, развитие инициативы в учебе и будущей деятельности в условиях рыночной экономики.

Для студентов, молодых ученых и преподавателей вузов.

Издательский дом «Плутон» www.idpluton.ru e-mail: admin@idpluton.ru

Подписано в печать 17.06.2019 г. Формат 14,8×21 1/4. | Усл. печ. л. 3.2. | Тираж 300.

Все статьи проходят рецензирование (экспертную оценку).

Точка зрения редакции не всегда совпадает с точкой зрения авторов публикуемых статей.

Авторы статей несут полную ответственность за содержание статей и за сам факт их публикации.

Редакция не несет ответственности перед авторами и/или третьими лицами и организациями за возможный ущерб, вызванный публикацией статьи.

При использовании и заимствовании материалов ссылка обязательна.

Оглавление

1. ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ СВЕРХПРОВОДЯЩИХ МАТЕРИАЛОВ В ЭНЕРГЕТИКЕ РОССИИ.....3
Елисеева А.А., Колесников Г.Ю., Щикунов Н.Н.
2. ФАЛЬСИФИКАЦИЯ МЯСНЫХ КОНСЕРВОВ ДЛЯ ДЛИТЕЛЬНОГО ХРАНЕНИЯ 6
Козлова А.Е., Солдатова С.Ю., Корзунов С.А.
3. КРИМИНАЛИЧЕСКОЕ ИССЛЕДОВАНИЕ ЖЕСТКОГО ДИСКА С УСТАНОВЛЕННОЙ ОПЕРАЦИОННОЙ СИСТЕМОЙ СЕМЕЙСТВА WINDOWS NT …….……..…9
Дмитрюк В.Л., Михайлов С.Ю., Иниватов Д.П., Киреев А.П.
4. ШТАТНЫЕ МЕХАНИЗМЫ ЗАЩИТЫ ИНФОРМАЦИИ И ЖУРНАЛИРОВАНИЯ СОБЫТИЙ БЕЗОПАСНОСТИ В ОС WINDOWS..... 16
Дмитрюк В.Л., Киреев А.П., Иниватов Д.П., Михайлов С.Ю.

Елисеева Анастасия Александровна
Eliseeva Anastasia Aleksandrovna
Старший преподаватель кафедры «Физики, электротехники и электроэнергетики»,
ФГАОУ ВО «Институт сервиса туризма и дизайна (филиал) СКФУ в г. Пятигорске»

Колесников Геннадий Юрьевич
Kolesnikov Gennady Yurevich
Кандидат технических наук, доцент кафедры «Физики, электротехники и электроэнергетики»,
ФГАОУ ВО «Институт сервиса туризма и дизайна (филиал) СКФУ в г. Пятигорске»

Щикунов Николай Николаевич
Shikunov Nikolay Nikolaevich
Студент кафедры «Физики, электротехники и электроэнергетики», инженерный факультет,
ФГАОУ ВО «Институт сервиса туризма и дизайна (филиал) СКФУ в г. Пятигорске»

УДК 621.31

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ СВЕРХПРОВОДЯЩИХ МАТЕРИАЛОВ В ЭНЕРГЕТИКЕ РОССИИ

PROSPECTS FOR THE USE OF SUPERCONDUCTORS MATERIALS IN THE ENERGY OF RUSSIA

Аннотация: Мир стоит на пороге «сверхпроводниковой» революции. По данным аналитических компаний, объёмы рынка сверхпроводниковых изделий стремительно растут. Эксперты говорят, что за этими технологиями – будущее энергетики. В России уже готов к промышленному использованию первый сверхпроводниковый ограничитель тока, который вскоре заработает на ПС 220 кВ Мнёвники в Москве

Abstract: The world is on the verge of a "superconducting" revolution. According to analytical companies, the market volume of superconducting products is growing rapidly. Experts say that behind these technologies is the future of energy. In Russia, the first superconducting current limiter is ready for industrial use, which will soon work at the 220 kV Mnevniki substation in Moscow

Ключевые слова: сверхпроводимость, сверхпроводящие материалы.

Key words: superconductivity, superconducting materials.

Сверхпроводимость - это свойство многих материалов иметь нулевое электрическое сопротивление, когда достигается критическая температура. Сверхпроводимость нашла очень много интересных применений в разных отраслях. Хранение и передача энергии являются составными частями этих применений.

Сверхпроводимость открыта Камерлинг-Оннесом в 1911 г., в ходе исследования электрических свойств металлов при низких температурах отмечено, что при температуре выше 4 тысяч кельвинов, сопротивление ртути становится нулевое. Спустя время, аналогичное явление удалось найти у 22 металлов. Сверхпроводящими являются многие сплавы, с температурами в ряде случаев более высокими, чем в моноатомных металлах.

Сверхпроводимость - это отсутствие сопротивления поэтому ток, возбужденный в сверхпроводящем контуре, не затухает в течение некоторого времени [1].

Одним из главных преимуществ некоторых сверхпроводящих материалов, является возможность достижения высокой плотности тока. Это важно, так как, чем выше плотность тока, тем приборы и устройства будут более компактными и легкими. В результате, уменьшается масса, которую необходимо охлаждать, а также уменьшается расход дорогостоящих сверхпроводящих материалов.

Пример, сверхпроводящие соленоиды для получения магнитного поля и кабели для передачи электрического тока в много раз меньше по объему и весу изготовленных из меди. Это позволяет снизить капитальные и эксплуатационные расходы установок, использующих сверхпроводники [2].

При изготовлении сверхпроводящего кабеля вокруг сверхпроводящего провода необходимо создать стабилизирующее покрытие из меди, которое обладает высокой тепло- и электропроводностью. Это делается для быстрого перевода электрического тока в медное покрытие и отвода тепла при случайном переходе сверхпроводника в нормальное состояние при пропускании высоких плотностей электрического тока [3].

Для повышения рабочих токов и как следствие достижение магнитных полей создают многожильные кабели энергии типа сверхпроводник-медь. При изготовлении таких кабелей в бруске меди круглого сечения просверливают отверстия, в которые запрессовываются тонкие стержни из сплава ниобия - титана. Получается композиционный брусок, который превращают в тонкие стержни, разрезают на куски, которые снова вставляют в новые бруски меди. Это операция повторяется многократно, в результате которой, получают кабель с большим числом сверхпроводящих жил, из которого затем наматывают катушки для сверхпроводящих соленоидов.

Куда более сложнее устроен высокотемпературный сверхпроводниковый кабель. Многослойная лента, которая выращивается на подложке из никелевого сплава при помощи ионного напыления.

В центральной части ленты имеется пленка из сверхпроводника толщиной около 2 микрон. Эта пленка окружена прослойками материалов, которые снижают степень ее зернистости при напылении и служит защитой от колебаний температуры. Толщина ленты в 100 раз превышает толщину сверхпроводящего слоя, поэтому она пропускает ток только в узкой центральной зоне.

Плюс ко всему для того чтобы увеличить максимальную плотность тока, в этот слой добавляют наночастицы. Поэтому изготовления такого кабеля длиной в один километр — это весьма трудоемкая и финансово-затратная задача.

Важной особенностью сверхпроводящих накопителей энергии, является запас энергии в магнитном поле индукционной катушки, где циркуляция тока происходит без потерь. Главным преимуществом такого накопителя является его быстродействие, которое достигается за доли миллисекунд, что позволяет быстро реагировать на внезапные аварии в энергосистеме [4].

Конструкцию таких накопителей, можно условно разделить на три составных части: магнитная система, криогенная система и система связи с внешней сетью. Данный метод накопления электроэнергии отличается чистой экологией, не используются вредные материалы, не происходит различных химических реакций, отсутствуют отходы производства.

Еще одной особенностью таких накопителей является длительное хранение энергии в форме магнитной энергии, это позволяет создавать системы с высоким уровнем готовности. Применение накопителей энергии в электроэнергетике позволяет решить две ключевые задачи: снизить затраты на производство электроэнергии и увеличить надежность энергосистем.

Постоянные (природные) магниты известны достаточно давно, но для большинства практических применений они непригодны. Не большая напряженность магнитного поля не может изменяться во времени из-за воздействия внешних факторов. Поэтому в 21 веке для получения магнитных полей используются электромагниты. Структура электромагнита выглядит следующим образом: провод, намотанный на сердечник, по которому течет ток. Магнитное поле, которое создается при этом пропорционально силе тока и количеству витков. Создание магнитов с большими напряженностями магнитного поля сопровождается увеличением силы тока и потерь энергии на теплоту Джоуля. Для создания крупных магнитов требуется водяное охлаждение, а получение напряженностей в десятки тысяч эрстед (сила напряженности) сложная задача без использования сверхпроводимости. В 21 веке серийно производятся многие виды сверхпроводящих магнитов, а также производятся на заказ для научных исследований и промышленного назначения.

Сегодня в мире задачами технической сверхпроводимости заняты множество научных коллективов. Сформулированы долгосрочные планы исследований, цели работ, подготовлены перечни объектов, подлежащих внедрению. В течении следующих нескольких лет будет осуществлен переход сверхпроводников из лабораторий в промышленность для крупномасштабных применений.

Библиографический список

1. В. Л. Гинзбург, Е. А. Андрюшин. Сверхпроводимость. — М.: Альфа-М, 2011.

2. «Сверхпроводимость: исследования и разработки» №6, 2009.-264 с.
3. Шмидт В.В. Введение в физику сверхпроводников. М.: Изд-во МЦНМО, 2010.
4. Мнеян М.Г. Сверхпроводники в современном мире. Книга для учащихся – М.: Просвещение, 2009.

Козлова Алевтина Евгеньевна
Kozlova Alevtina Evgenevna
старший научный сотрудник, ФГБУ Научно-исследовательский институт проблем хранения Росрезерва, г.Москва

Солдатова Светлана Юрьевна
Soldatova Svetlana Yuryevna
старший научный сотрудник, ФГБУ Научно-исследовательский институт проблем хранения Росрезерва, г.Москва

Корзунов Сергей Александрович
Korzunov Sergey Aleksandrovich
главный специалист ФГБУ Научно-исследовательский институт проблем хранения Росрезерва, г.Москва

УДК 664.93

ФАЛЬСИФИКАЦИЯ МЯСНЫХ КОНСЕРВОВ ДЛЯ ДЛИТЕЛЬНОГО ХРАНЕНИЯ

FALSIFICATION OF MEAT CANNED FOOD FOR LONG STORAGE

Аннотация: Мясные консервы продукт, который в последнее время все чаще подвергается фальсификации. В статье представлена информация по методам исследования фальсификации мясных консервов.

Abstract: Canned meat is a product that has recently been increasingly subjected to falsification. The article presents information on methods of research of falsification of canned meat.

Ключевые слова: Мясные консервы, фальсификация, мясо, мясная продукция.

Keywords: Fish Canned meat, falsification, meat, meat products.

Введение

Развитие современной мясной промышленности связано с производством продуктов не только кратковременного, но и длительного срока годности, при котором осуществляется наиболее эффективное использование мясного сырья. К такому виду продукции относятся стерилизованные мясные консервы, основное преимущество которых заключается в возможности длительного хранения без потерь питательных и вкусовых качеств. Возможность фальсификации мяса и мясной продукции появяется в результате отсутствия стандартизованных современных эффективных методов исследования. Для выявления фальсифицированной продукции недостаточно установления ее соответствия существующим требованиям качества и безопасности. Идентификация происхождения сырья для производства пищевых продуктов – это наиболее актуальный вопрос при разработке подходов к выявлению фальсификации и более полной оценке его качества.

Объекты и методы исследований.

В качестве объекта исследований взяты опытные образцы консервов мясных кусковых стерилизованных «Говядина тушеная высший сорт» по ГОСТ 32125-2013, масса нетто 338 г. различных производителей приобретенные в торговой сети: образец № 1- производитель: ООО «БРТ», образец № 2- производитель: ООО «Орелпродукт», образец № 3- производитель: ЗАО «Лыткаринский МПЗ».

В работе использованы следующие методы определения:

— массовая доля белка по методу Къельдаля[1].

— величины кислотного (КЧ) числа — титрометрическим методом, основанным на титровании свободных жирных кислот раствором гидроокиси калия [2];

— величины перекисного (ПЧ) числа жира по реакции взаимодействия продуктов окисления животных жиров (перекисей и гидроперекисей) с йодистым калием в растворе уксусной кислоты и хлороформа с последующим количественным определением выделившегося йода раствором тиосульфата натрия титриметрическим методом [3];

Перекисное и кислотное числа определялись как дополнительные показатели для выявление качества сырья, согласно требованиям ГОСТ 34177-2017 п.5.3[4].

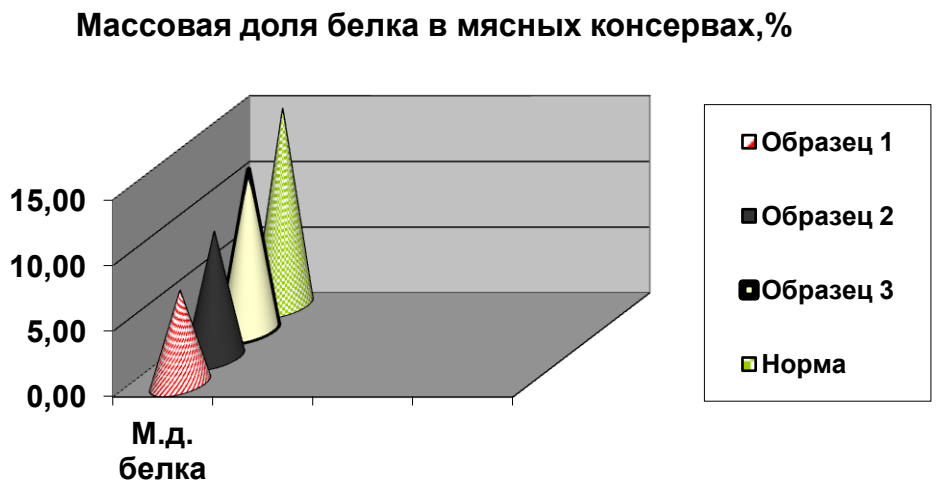


Рис. 1 - Массовая доля белка в консервах мясных кусковых

Сравнительный анализ содержания массовой дли белка 3-х образцов приобретенных в торговой сети показал, что образцы не отвечают требованиям ГОСТ 32125-2013(м.д. белка не менее 15%) и могут рассматриваться как фальсификация продукции.

На основании ранее проведенных исследований предельно допустимое значение перекисного числа было принято 10 (моль(1/2О/кг), а кислотного 4 мг КОН/г.

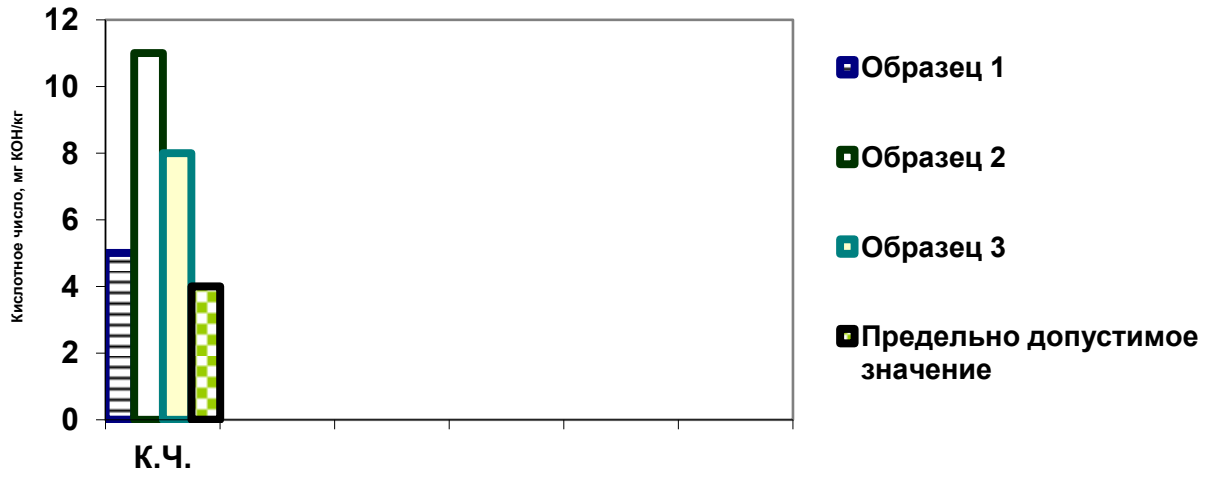


Рис.2 – Значение кислотного числа в консервах мясных кусковых

Результаты испытаний показали, что все три образца выходили за нормы предельно допустимого значения. Значение образца №1- 5±0,1 мг КОН/г, образца № 2-11±0,1, образца №3-8±0,1 , что превышает предельно допустимое значение.

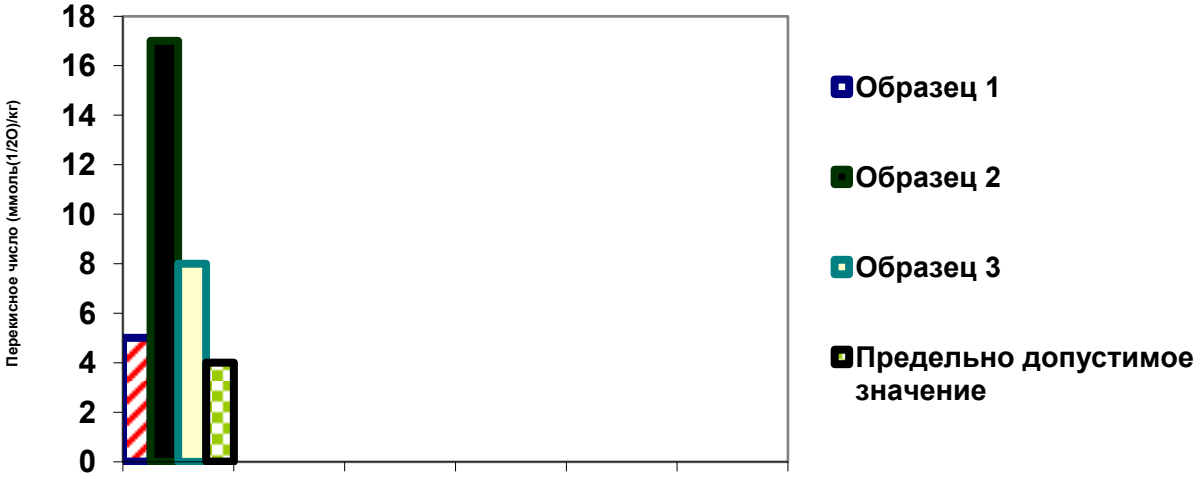


Рис.3 - Значение перекисного числа в консервах мясных кусковых

Значение образца №1- 6,0±1,6 (моль(1/2О/кг). Образца № 2-17,0±4,6(моль(1/2О/кг), образца №3- 12,0±3,2(моль(1/2О/кг), что превышает предельно допустимое значение.

В заключение надо сказать, что методы анализа, включенные в действующую нормативную документацию, позволяют контролировать, но отсутствие четкого, регламентированного нормативной документацией определения фальсификации мяса, как и других пищевых продуктов, существенно осложняет выявление факта фальсификации и зачастую делает невозможным его документальное подтверждение. Для выявления фальсификации мяса и мясной продукции необходимы современные научно- методические подходы, а также совершенствование и гармонизация нормативной документации.

Библиографический список:

1. ГОСТ 25011-2017 Мясо и мясные продукты. Методы определения белка http://docs.cntd.ru/document/1200146783.

2. ГОСТ Р 55480-2013 Мясо и мясные продукты. Метод определения кислотного числа http://docs.cntd.ru/document/1200103311.

3. ГОСТ 34118-2017 Мясо и мясные продукты. Метод определения перекисного числа http://docs.cntd.ru/document/1200146654.

4. ГОСТ 34177-2017 Консервы мясные. Общие технические условия. http://docs.cntd.ru/document/556309635.

Дмитрюк Вячеслав Леонидович
старший преподаватель, Омский государственный технический университет, Россия, г. Омск
Михайлов Сергей Юрьевич
студент Радиотехнического факультета Омского государственного технического университета, Россия, г. Омск
Иниватов Даниил Павлович
студент Радиотехнического факультета Омского государственного технического университета, Россия, г. Омск
Киреев Александр Павлович
студент Радиотехнического факультета Омского государственного технического университета, Россия, г. Омск

Dmitriyuk Vyacheslav Leonidovich
Senior Lecturer, Omsk State Technical University, Russia, Omsk
Mikhailov Sergey Yurievich
Student, Radio Engineering Faculty, Omsk State Technical University, Russia, Omsk
Iniwatov Daniil Pavlovich
Student, Radio Engineering Faculty, Omsk State Technical University, Russia, Omsk
Kireev Alexander Pavlovich
Student, Radio Engineering Faculty, Omsk State Technical University, Russia, Omsk

УДК 004.032:343.98

КРИМИНАЛИЧЕСКОЕ ИССЛЕДОВАНИЕ ЖЕСТКОГО ДИСКА С УСТАНОВЛЕННОЙ ОПЕРАЦИОННОЙ СИСТЕМОЙ СЕМЕЙСТВА WINDOWS NT

CRIMINAL STUDY OF A HARD DRIVE WITH AN INSTALLED OPERATING SYSTEM OF THE WINDOWS NT FAMILY

Аннотация: в ходе данной статьи проведен поэтапный криминалистический анализ жесткого диска с предустановленной операционной системой семейства Windows NT.

Abstract: in the course of this article, a phased forensic analysis of a hard disk with a preinstalled operating system of the Windows NT family was carried out.

Ключевые слова: операционная система, криминалистический анализ, исследование, артефакты, программное обеспечение.

Keywords: operating system, forensic analysis, research, artifacts, software.

АНАЛИЗ ОБРАЗА НАРУШИТЕЛЯ

Для анализа содержимого исследуемого образа воспользуемся рекомендованным программным обеспечением для расследования компьютерных преступлений: ***OSForensic, Belkasoft.*** Также по мере необходимости интегрируем дополнительный софт.

Описание объекта исследования.

Для получения характеристик исследуемого образа воспользуемся программным обеспечением для расследования компьютерных преступлений. Попробуем определить данные характеристики с помощью OSForensic. На Рис. 1. отчетливо видно, что данное ПО не способно вывести системную информацию (System Information) Image-файла (образа).

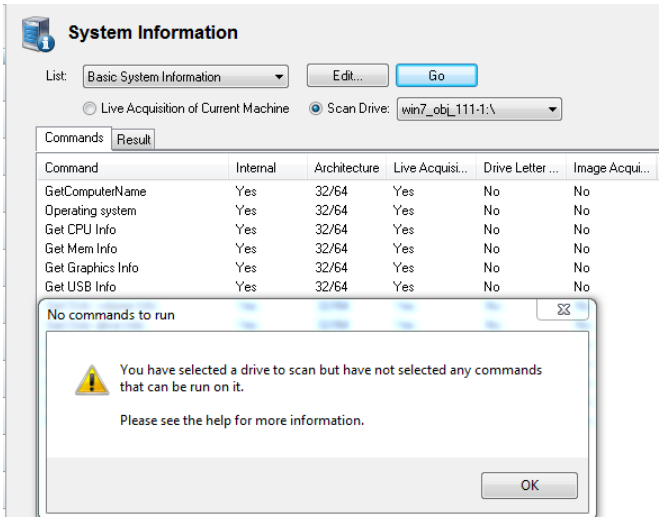


Рис. 1. Ошибка при получении системной информации с помощью OSForensic

При помощи программного обеспечения BelkaSoft можно сделать вывод о том, что формат данного диска NTFS. Также к данному выводу можно прийти путем подключения виртуального жесткого диска:

Компьютер – Управление – Управление дисками – Действие – Присоединить виртуальный жесткий диск.

Также можно судить о том, что исследуемый образ состоит из 2-х логических разделов, один из которых зарезервирован системой (Рис. 2).

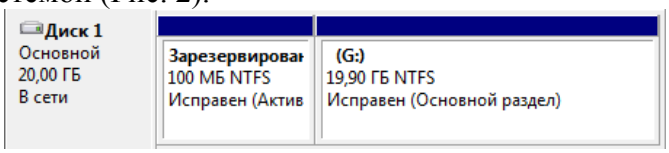


Рис. 2. Логические разделы исследуемого образа

Если смонтировать данный образ, например, при помощи свободно распространяемого ПО ***FTK Imager***, то можно обнаружить тот факт, что файловая структура соответствует операционной системе Windows.

Определим, какие учетные записи предоставлены на данном образе. Для этого воспользуемся программой ***OSForensic***. Перейдем во вкладку «Password», после чего «Windows Login Password». Выберем исследуемый образ и нажмем кнопку «Acquire Password». Результатом будет служить таблица с учетными записями и их паролями (либо хэшами паролей) (Рис. 3).

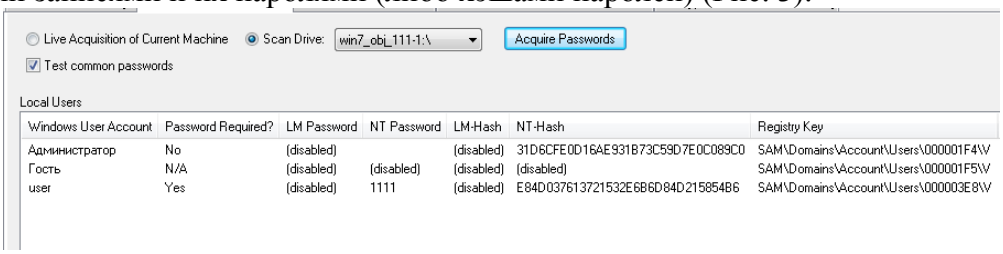


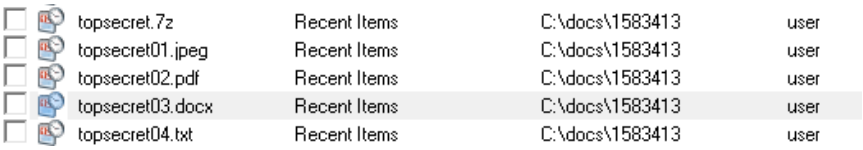
Рис. 3. Список учетных записей исследуемого образа

Получим список установленного программного обеспечения. Для этого перейдем непосредственно к смонтированному образу. В результате анализа были выявлены следующие программы: Wireshark, Mozila Firefox, Mozila Maintenance Service (обновление браузера), Mozila Thunderbird (электронная почта), WinPcap (программы анализа сетевых данных), VirtualBox. Также посредством анализа графический файлов (полученных в процессе карвинга), содержащихся на исследуемом носители, было обнаружено использование следующих программ: Skype, Agent mail.ru, ICQ. Данный нуждаются в последующем анализе.

Для определения отправной точки исследования проанализируем последнюю активность пользователя. Перейдем в OSForensic – Recent Activity – Выбираем исследуемый образ – Scan (Рис. 4).

Рис. 4. Результаты исследования последней активности пользователя

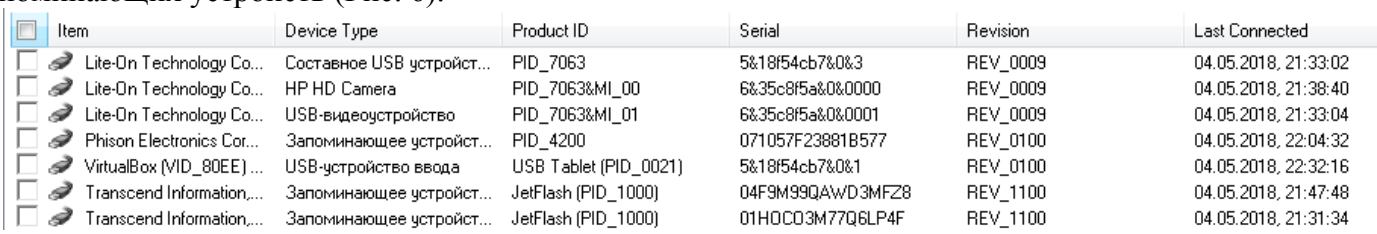
Из исследования недавно открытых документов видно, что они, в свою очередь, хранились в директории C:\docs\1583413. (Рис. 5) Пройдя по данной директории, можем обнаружить, что она не существует. Следовательно, пользователь удалил папку. Можно сделать вывод о том, что для полного исследования образа необходимо воспользоваться сторонним ПО для восстановления и анализа удаленных файлов.



topsecret.7z	Recent Items	C:\docs\1583413	user
topsecret01.jpeg	Recent Items	C:\docs\1583413	user
topsecret02.pdf	Recent Items	C:\docs\1583413	user
topsecret03.docx	Recent Items	C:\docs\1583413	user
topsecret04.txt	Recent Items	C:\docs\1583413	user

Рис. 5. Анализ недавно открытых документов

Проанализируем USB-устройства. Для этого необходимо перейти: OSForensic – Recent Activity – USB. В полученном результате видим, что данный образ является виртуальным жестким диском, на компьютере присутствовала видеокамера, а также то, что было подключение сторонних запоминающих устройств (Рис. 6).



Item	Device Type	Product ID	Serial	Revision	Last Connected
Lite-On Technology Co...	Составное USB устройст...	PID_7063	5&18f54cb7&0&3	REV_0009	04.05.2018, 21:33:02
Lite-On Technology Co...	HP HD Camera	PID_7063&MI_00	6&35c8f5a&0&0000	REV_0009	04.05.2018, 21:38:40
Lite-On Technology Co...	USB-видеоустройство	PID_7063&MI_01	6&35c8f5a&0&0001	REV_0009	04.05.2018, 21:33:04
Phison Electronics Cor...	Запоминающее устройст...	PID_4200	071057F23881B577	REV_0100	04.05.2018, 22:04:32
VirtualBox (VID_80EE) ...	USB-устройство ввода	USB Tablet (PID_0021)	5&18f54cb7&0&1	REV_0100	04.05.2018, 22:32:16
Transcend Information,...	Запоминающее устройст...	JetFlash (PID_1000)	04F9M99QAWD3MFZ8	REV_1100	04.05.2018, 21:47:48
Transcend Information,...	Запоминающее устройст...	JetFlash (PID_1000)	01HOCO3M77Q6LP4F	REV_1100	04.05.2018, 21:31:34

Рис. 6. Анализ USB-устройств

Выполним анализ Интернет-активности в браузере. Отчётливо видим, что подозреваемый пользовался почтой (mail.ru), скачивал браузер Mozila Firefox, пользовался облаком mail.ru, заходил на сайт и скачивал ICQ (подтверждение вышесказанному), Wireshark, Thunderbird. Также было выявлено обращение к другим сторонним веб-ресурсам (Рис. 7).

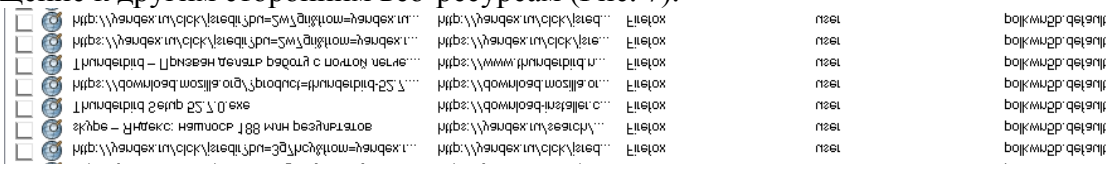


Рис. 7. Анализ веб-активности

Пользуясь средствами OSForensic проанализируем удаленные файлы. Для этого перейдем во вкладку «Deleted Files Search», выберем исследуемый носитель и нажмем на кнопку «Search». Результат анализа показал, что среди удаленных файлов, скорее всего, нет тех, которые необходимы для исследования (Рис. 8).

0000000000000372	win7_obj_111-1:\$Extend\$RmMetadata\$Txf\	221.0 KB	Файл
0000000000000373	win7_obj_111-1:\$Extend\$RmMetadata\$Txf\	4.15 MB	Файл
0000000000000374	win7_obj_111-1:\$Extend\$RmMetadata\$Txf\	24.42 MB	Файл
aborted-session-ping	win7_obj_111-1:\Users\user\AppData\Roaming...	24.34 KB	Файл
EtwRTEventlog-Securit...	win7_obj_111-1:\Windows\System32\LogFiles\...	72 Bytes	Файл "ETL"
EtwRTUBPM.etl	win7_obj_111-1:\Windows\System32\LogFiles\...	72 Bytes	Файл "ETL"
prefs.js	win7_obj_111-1:\Users\user\AppData\Roaming...	8.72 KB	Файл сценари...
recovery.baklz4	win7_obj_111-1:\Users\user\AppData\Roaming...	14.84 KB	Файл "BAKLZ4"
sessionCheckpoints.json	win7_obj_111-1:\Users\user\AppData\Roaming...	90 Bytes	JSON File
test-harmful-simple.sbst...	win7_obj_111-1:_unknown_\	232 Bytes	Файл "SBSTO...
test-malware-simple.sbs...	win7_obj_111-1:_unknown_\	232 Bytes	Файл "SBSTO...
test-unwanted-simple.p...	win7_obj_111-1:_unknown_\	16 Bytes	Файл "PSET"
tmp.edb	win7_obj_111-1:\ProgramData\Microsoft\Searc...	8.06 MB	Файл "EDB"
xulstore.json	win7_obj_111-1:\Users\user\AppData\Roaming...	203 Bytes	JSON File

Рис. 8. Список недавно удаленных файлов

Перейдем в программное обеспечение BelkaSoft. Первым делом определим, с какими пользователями общался подозреваемый посредством использования электронной почты. Результаты анализа следующие: подозреваемый общался только с одним пользователем. E-mail подозреваемого: azuev1981@mail.ru. E-mail единственного пользователя: webmaster13@mail.ru (Рис. 9).

webmaster13@mail.ru	Sender UIN	azuev1981@mail...	InstantMessen...	win7_obj_111.vmdk
azuev1981@mail.ru	Receiver UIN	azuev1981@mai...	InstantMessen...	win7_obj_111.vmdk
webmaster13@mail.ru	Sender UIN	azuev1981@mai...	InstantMessen...	win7_obj_111.vmdk
azuev1981@mail.ru	Receiver UIN	azuev1981@mai...	InstantMessen...	win7_obj_111.vmdk
webmaster13@mail.ru	Sender UIN	azuev1981@mai...	InstantMessen...	win7_obj_111.vmdk
azuev1981@mail.ru	Receiver UIN	azuev1981@mai...	InstantMessen...	win7_obj_111.vmdk
webmaster13@mail.ru	Sender UIN	azuev1981@mai...	InstantMessen...	win7_obj_111.vmdk

Рис. 9. Адреса e-mail

Обнаруженные файлы с данным флагом

Путем длительного анализа были выявлены следующие файлы, содержащие конфиденциальную информацию: topsecret.7z (архив), topsecret01.jpeg, topsecret02.pdf, topsecret03.doc, topsecret04.txt. Так как образ содержал три файла с конфиденциальной информации, то можно предположить, что topsecret.7z не содержит уникальных файлов и был создан для отправки во внешнюю сеть. Остается 4 файла, три из которых конфиденциальны. Имеет место предположение, что при создании doc-документа, автоматически создается резервный документ – txt (предположение). Таким образом, задача сводится к поиску txt, jpeg, pdf.

После обработки массива данных был найден pdf-документ (Рис. 10).

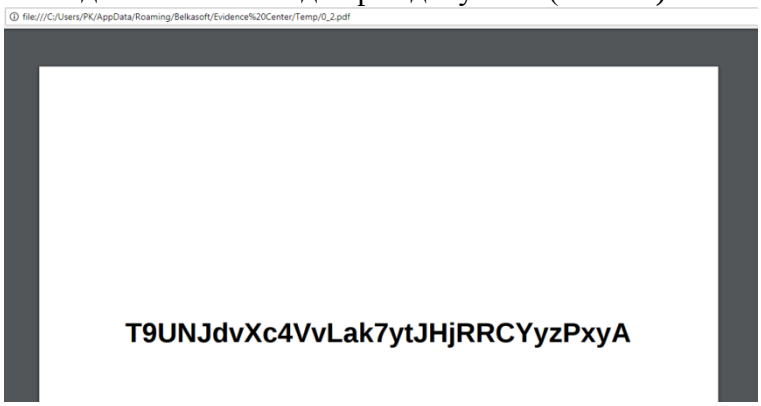


Рис. 10. Pdf-документ, содержащий конфиденциальную информацию

С помощью интегрированного программного обеспечения Hetman PR было обнаружено изображение, содержащее конфиденциальную информацию (Рис. 11). Данный файл предоставляет собой иконку, поэтому имеет низкое качество. Но необходимый ключ разглядеть вполне реально.

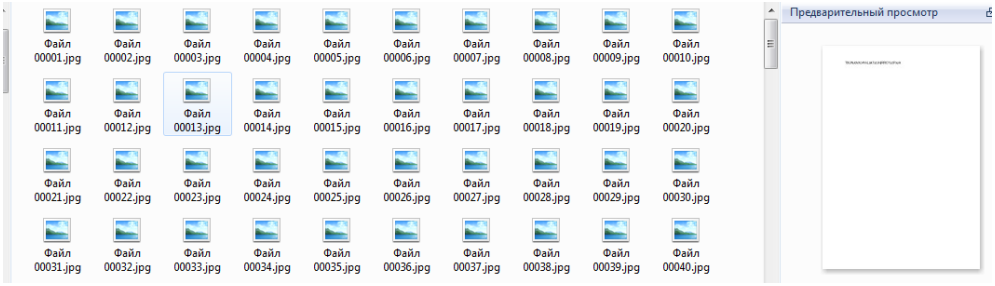


Рис. 11. Jpeg-документ, содержащий конфиденциальную информацию

Аналогичного результата удалось достичь путем просмотра сообщений, отправленных с помощью ПО ICQ. Но в данном случае качество картинки заметно лучше (Рис. 12).

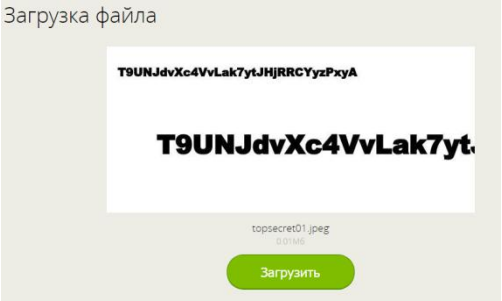


Рис. 12. Jpeg-документ, содержащий конфиденциальную информацию

После досконального и длительного исследования образа текстовый файл найти не удалось. Использовались как программы для сортировки данных по расширениям (в том числе собственно написанный скрипт), так и программы для поиска удаленных файлов.

Таким образом, было обнаружено 2 файла, содержащие конфиденциальные сведения. Также были найдены каналы, по которым данные отправлялись во внешнюю сеть, а именно: посредством ICQ и электронной почты (Рис. 13, 14).

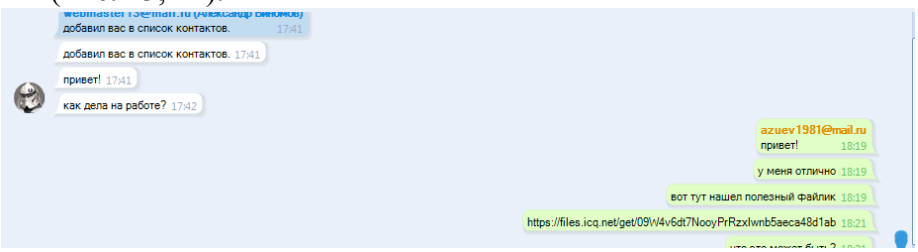


Рис. 13. Утечка посредством ICQ

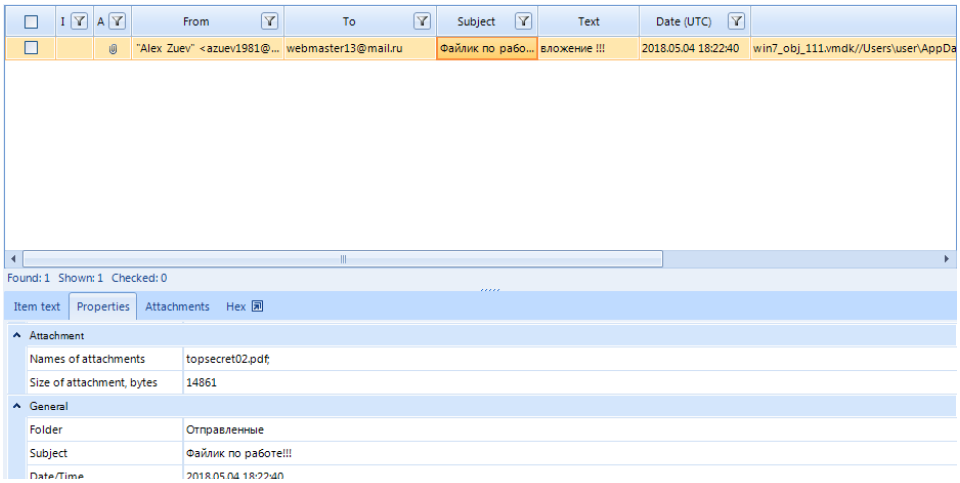


Рис. 14. Утечка посредством отправки e-mail письма

АНАЛИЗ WIRESHARK

Для анализа дампа Wireshark было использовано стороннее программное обеспечение ***NetworkMinner***. Из первого пункта известно, что один из конфиденциальных файлов передавался

посредством ICQ. Номер порта, использующий ICQ, 5050, 5190. Отфильтровав трафик Wireshark по данному порту, обнаружим, что фильтрованный список пуст (Рис. 15). Это означает тот факт, что приложение ICQ на исследуемый ПК не устанавливалось – использовалась WEB-версия приложения.

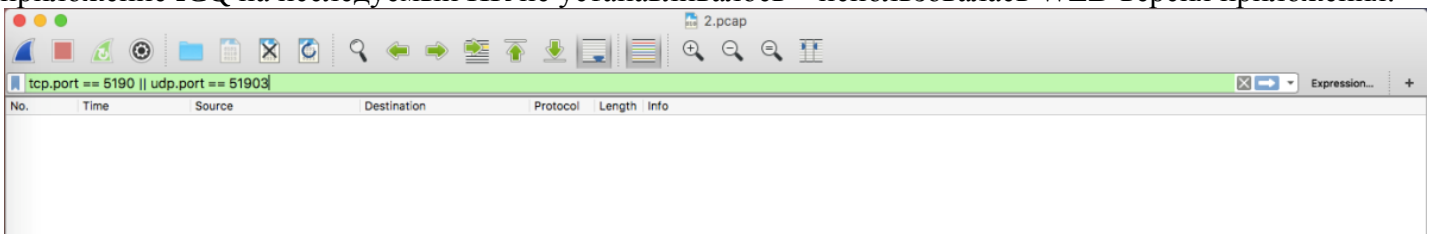


Рис. 15. Отфильтрованный трафик Wireshark

Следовательно, трафик отправлялся посредством веб-браузера через протокол 80 (HTTP), 443 (HTTPS). Из рис. 16 можно видеть, что нарушитель общался с единственным контактом, адрес которого 94.100.180.90. Можно предположить, что Ip-адрес данного контакта не изменялся, следовательно, и данные через ICQ были переданы с этого же адреса.

Item...	Text	Field name	Profile name	Profile type	Source
	ogon.exe **127.0.0.1** 0	Description	System event logs	SystemEventL...	win7_obj_111.vmdk
	ogon.exe **127.0.0.1** 0	Description	System event logs	SystemEventL...	win7_obj_111.vmdk
	1g3e.inf **8.4.1.0** Microsoft PCI\VEN_8086'DEV_100E'SUBSYS_001E8086	Description	System event logs	SystemEventL...	win7_obj_111.vmdk
	.0.0:123-> **52.178.161.41** :123)	Description	System event logs	SystemEventL...	win7_obj_111.vmdk
	.0.0:123-> **52.178.161.41** :123)	Description	System event logs	SystemEventL...	win7_obj_111.vmdk
	uest.inf **5.1.34.0** Oracle Corporation PCI\VEN_80EE'DEV_CAFE'SUBSYS_	Description	System event logs	SystemEventL...	win7_obj_111.vmdk
	ideo.inf **5.1.34.0** Oracle Corporation PCI\VEN_80EE'DEV_BEEF'SUBSYS_	Description	System event logs	SystemEventL...	win7_obj_111.vmdk
	00080G541h:::	Value	image:\2\vol_10...	Browser	win7_obj_111.vmdk
	ved: from **46.233.195.90** :55374 by 94.100.180.90:993 with IMAP Fri, 04 May 2018 1	HTTP headers	jrxy1tzm.default	Mail	win7_obj_111.vmdk

Рис. 16. Ip-адрес нарушителя

Отфильтровав трафик по ip-адресу, видим совокупность пакетов. Прочитать их не предоставляется возможным, так как данные зашифрованы (Рис. 17).

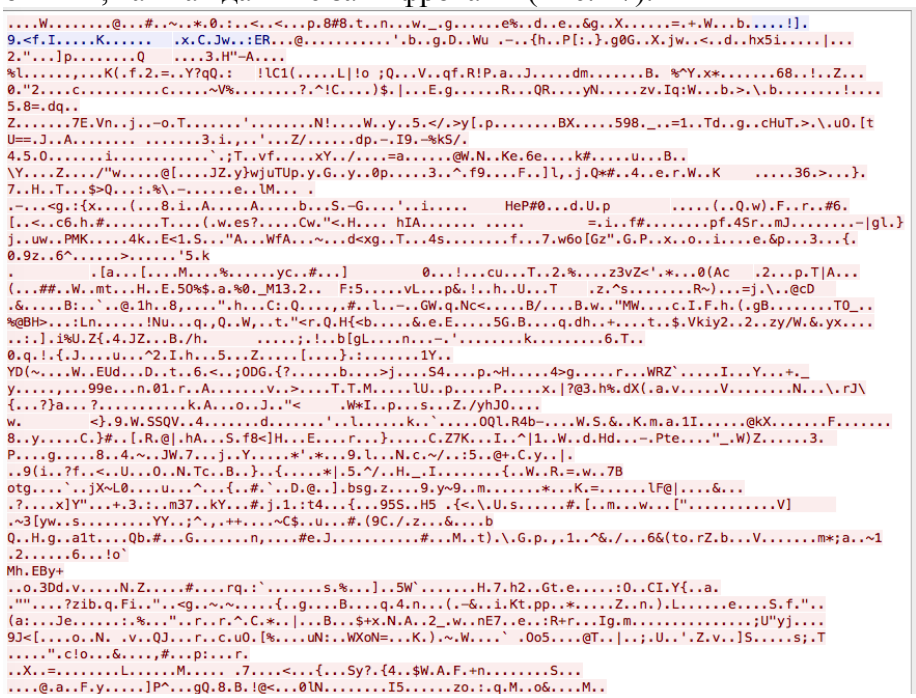


Рис. 17. Шифрованный трафик Wireshark

Из рис. 18 видно, что нарушитель и пользователь общались посредством электронной почты через 993 порт (с данного порта отправлялись данные, на 55374 порт данные присылались). Воспользуемся этим. Отфильтруем трафик посредством 993 порта (Рис. 20). Просмотреть данный трафик так же не предоставляется возможным, так как данные зашифрованы.

tcp.port == 993 || udp.port == 993

No.	Time	Source	Destination	Protocol	Length	Info
1924	234.365434	10.0.2.15	94.100.180.90	TLSv1…	146	Application Data
1925	234.365747	94.100.180.90	10.0.2.15	TCP	60	993 → 49204 [ACK] Seq=1 Ack=93 Win=65535 Len=0
1926	234.399245	94.100.180.90	10.0.2.15	TLSv1…	92	Application Data
1927	234.432213	10.0.2.15	94.100.180.90	TCP	2974	49204 → 993 [ACK] Seq=93 Ack=39 Win=63320 Len=2920 [TCP segment of a reassembled PDU]
1928	234.432464	94.100.180.90	10.0.2.15	TCP	60	993 → 49204 [ACK] Seq=39 Ack=3013 Win=65535 Len=0
1929	234.432481	10.0.2.15	94.100.180.90	TCP	5894	49204 → 993 [ACK] Seq=3013 Ack=39 Win=63320 Len=5840 [TCP segment of a reassembled PDU]
1930	234.432819	94.100.180.90	10.0.2.15	TCP	60	993 → 49204 [ACK] Seq=39 Ack=4473 Win=65535 Len=0
1931	234.432820	94.100.180.90	10.0.2.15	TCP	60	993 → 49204 [ACK] Seq=39 Ack=5933 Win=65535 Len=0
1932	234.432843	10.0.2.15	94.100.180.90	TCP	5894	49204 → 993 [ACK] Seq=8853 Ack=39 Win=63320 Len=5840 [TCP segment of a reassembled PDU]
1933	234.432913	94.100.180.90	10.0.2.15	TCP	60	993 → 49204 [ACK] Seq=39 Ack=7393 Win=65535 Len=0
1934	234.432914	94.100.180.90	10.0.2.15	TCP	60	993 → 49204 [ACK] Seq=39 Ack=8853 Win=65535 Len=0
1935	234.432929	10.0.2.15	94.100.180.90	TLSv1…	1867	Application Data
1936	234.433011	94.100.180.90	10.0.2.15	TCP	60	993 → 49204 [ACK] Seq=39 Ack=10313 Win=65535 Len=0
1937	234.433011	94.100.180.90	10.0.2.15	TCP	60	993 → 49204 [ACK] Seq=39 Ack=11773 Win=65535 Len=0
1938	234.433012	94.100.180.90	10.0.2.15	TCP	60	993 → 49204 [ACK] Seq=39 Ack=13233 Win=65535 Len=0
1939	234.433012	94.100.180.90	10.0.2.15	TCP	60	993 → 49204 [ACK] Seq=39 Ack=14693 Win=65535 Len=0

Рис. 18. Фильтрация по 993 порту

В аудитории было сказано, что один из каналов передачи не шифруется. Так как всего имеем 3 канала утечки, два из которых успешно обнаружены, делаем вывод, что последний файл с конфиденциальной информацией передавался в открытом виде без шифрования. То есть мы можем посмотреть содержимое файла. Для этого воспользуемся программой для сортировки трафика NetworkMonitor. Загрузим дамп, после чего перейдем во вкладку «Files». В данном разделе содержатся файлы формата png, jpg (картинки), cer (сертификат), txt (текстовый файл) и другие (Рис. 19). Проанализировав каждый из файлов, делаем вывод о том, что среди нет отсутствует конфиденциальный файл, так как нигде не обнаружен заданный флаг.

Hosts (431) | Files (741) | Images (24) | Messages | Credentials (4) | Sessions (505) | DNS (1915) | Parameters (16218) | Keywords | Anomalies

Filter keyword: Case sensitive ExactPhrase Any column Clear Apply

Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host	D. port	Protocol	Time
26446	sync.republer.com.cer	cer	1 371 B	194.190.117.32 [ssp.republer.com] [sync.republer.com] (Ot…	TCP 443	10.0.2.15 (Windows)	TCP 49845	TlsCertificate	2018
26446	COMODO RSA Domain Validation.cer	cer	1 548 B	194.190.117.32 [ssp.republer.com] [sync.republer.com] (Ot…	TCP 443	10.0.2.15 (Windows)	TCP 49845	TlsCertificate	2018
26446	COMODO RSA Certification Aut.cer	cer	1 400 B	194.190.117.32 [ssp.republer.com] [sync.republer.com] (Ot…	TCP 443	10.0.2.15 (Windows)	TCP 49845	TlsCertificate	2018
26512	audtd.com[3].cer	cer	1 357 B	78.155.222.215 [pool2.audsp.com] [sync.audtd.com] [sync…	TCP 443	10.0.2.15 (Windows)	TCP 49847	TlsCertificate	2018
26512	COMODO RSA Domain Validation[3].cer	cer	1 548 B	78.155.222.215 [pool2.audsp.com] [sync.audtd.com] [sync…	TCP 443	10.0.2.15 (Windows)	TCP 49847	TlsCertificate	2018
26512	COMODO RSA Certification Aut[3].cer	cer	1 400 B	78.155.222.215 [pool2.audsp.com] [sync.audtd.com] [sync…	TCP 443	10.0.2.15 (Windows)	TCP 49847	TlsCertificate	2018
26512	AddTrust External CA Root[3].cer	cer	1 082 B	78.155.222.215 [pool2.audsp.com] [sync.audtd.com] [sync…	TCP 443	10.0.2.15 (Windows)	TCP 49847	TlsCertificate	2018
26541	adriver.ru.cer	cer	1 197 B	195.209.111.16 [ssp.adriver.ru] (Other)	TCP 443	10.0.2.15 (Windows)	TCP 49848	TlsCertificate	2018
26541	RapidSSL RSA CA 2018.cer	cer	1 205 B	195.209.111.16 [ssp.adriver.ru] (Other)	TCP 443	10.0.2.15 (Windows)	TCP 49848	TlsCertificate	2018
17123	styles.css	css	45 748 B	5.45.122.97 [telegram.org.ru] (Other)	TCP 80	10.0.2.15 (Windows)	TCP 49730	HttpGetChunked	2018
17131	rrssb.css	css	7 892 B	5.45.122.97 [telegram.org.ru] (Other)	TCP 80	10.0.2.15 (Windows)	TCP 49728	HttpGetChunked	2018
17132	font-awesome.min.css	css	31 000 B	5.45.122.97 [telegram.org.ru] (Other)	TCP 80	10.0.2.15 (Windows)	TCP 49731	HttpGetChunked	2018
17124	engine.css	css	63 887 B	5.45.122.97 [telegram.org.ru] (Other)	TCP 80	10.0.2.15 (Windows)	TCP 49729	HttpGetChunked	2018
17184	styles.css	css	2 187 B	5.45.122.97 [telegram.org.ru] (Other)	TCP 80	10.0.2.15 (Windows)	TCP 49730	HttpGetChunked	2018
17306	style.css	css	34 594 B	5.45.122.97 [telegram.org.ru] (Other)	TCP 80	10.0.2.15 (Windows)	TCP 49730	HttpGetChunked	2018
18081	comment2.css.3E1C7F62.css	css	47 524 B	136.243.130.80 [h.cackle.me] (Other)	TCP 80	10.0.2.15 (Windows)	TCP 49741	HttpGetChunked	2018
18494	hit.C0089A76.gif	gif	140 B	88.212.196.66 [counter.yadro.ru] (Other)	TCP 80	10.0.2.15 (Windows)	TCP 49751	HttpGetNormal	2018
2323	index.html	html	37 B	217.69.139.200 [mail.ru] (Other)	TCP 80	10.0.2.15 (Windows)	TCP 49391	HttpGetNormal	2018
17049	4403-kak-oboyti.html	html	40 450 B	5.45.122.97 [telegram.org.ru] (Other)	TCP 80	10.0.2.15 (Windows)	TCP 49726	HttpGetChunked	2018
18342	favicon.ico	ico	3 638 B	5.45.122.97 [telegram.org.ru] (Other)	TCP 80	10.0.2.15 (Windows)	TCP 49729	HttpGetNormal	2018
17394	1521672330_7b60526702.jpg	jpg	17 562 B	5.45.122.97 [telegram.org.ru] (Other)	TCP 80	10.0.2.15 (Windows)	TCP 49726	HttpGetChunked	2018
17409	1521672342_photo.jpg	jpg	17 428 B	5.45.122.97 [telegram.org.ru] (Other)	TCP 80	10.0.2.15 (Windows)	TCP 49732	HttpGetChunked	2018
17395	1521672387_78a340c6dd.jpg	jpg	18 739 B	5.45.122.97 [telegram.org.ru] (Other)	TCP 80	10.0.2.15 (Windows)	TCP 49731	HttpGetChunked	2018
17392	1521675955_vpn.jpg	jpg	31 542 B	5.45.122.97 [telegram.org.ru] (Other)	TCP 80	10.0.2.15 (Windows)	TCP 49729	HttpGetChunked	2018
17393	1521675696_proxy.jpg	jpg	33 049 B	5.45.122.97 [telegram.org.ru] (Other)	TCP 80	10.0.2.15 (Windows)	TCP 49730	HttpGetChunked	2018
17404	1521672439_d787176f86.jpg	jpg	18 609 B	5.45.122.97 [telegram.org.ru] (Other)	TCP 80	10.0.2.15 (Windows)	TCP 49728	HttpGetChunked	2018
17430	1521672370_photo.jpg	jpg	22 142 B	5.45.122.97 [telegram.org.ru] (Other)	TCP 80	10.0.2.15 (Windows)	TCP 49726	HttpGetChunked	2018
17455	1521672371_photo.jpg	jpg	21 737 B	5.45.122.97 [telegram.org.ru] (Other)	TCP 80	10.0.2.15 (Windows)	TCP 49732	HttpGetChunked	2018
17537	1521672393_photo.jpg	jpg	26 025 B	5.45.122.97 [telegram.org.ru] (Other)	TCP 80	10.0.2.15 (Windows)	TCP 49730	HttpGetChunked	2018
17554	1521672412_photo.jpg	jpg	24 573 B	5.45.122.97 [telegram.org.ru] (Other)	TCP 80	10.0.2.15 (Windows)	TCP 49729	HttpGetChunked	2018
17556	1521672408_photo.jpg	jpg	21 074 B	5.45.122.97 [telegram.org.ru] (Other)	TCP 80	10.0.2.15 (Windows)	TCP 49731	HttpGetChunked	2018

Рис. 19. Анализ переданных файлов

ЗАКЛЮЧЕНИЕ

Таким образом, были рассмотрены и изучены основные программы для расследования компьютерных преступлений, проанализирован учебный образ нарушителя.

Также был задействован и проанализирован дамп сетевой активности, полученный путем сбора трафика программным обеспечением Wireshark.

Библиографический список

1. Пархомов В. А. К определению понятия «информационное преступление» // Вестник Иркутской государственной экономической академии. — 2001. — No 1. — С. 92–96.

2. Федотов Н. Н. Форензика — компьютерная криминалистика. — М., 2007. — С. 129.

Дмитрюк Вячеслав Леонидович
старший преподаватель, Омский государственный технический университет, Россия, г. Омск
Киреев Александр Павлович
студент Радиотехнического факультета Омского государственного технического университета, Россия, г. Омск
Иниватов Даниил Павлович
студент Радиотехнического факультета Омского государственного технического университета, Россия, г. Омск
Михайлов Сергей Юрьевич
студент Радиотехнического факультета Омского государственного технического университета, Россия, г. Омск

Dmitriyuk Vyacheslav Leonidovich
Senior Lecturer, Omsk State Technical University, Russia, Omsk
Kireev Alexander Pavlovich
Student, Radio Engineering Faculty, Omsk State Technical University, Russia, Omsk
Iniwatov Daniil Pavlovich
Student, Radio Engineering Faculty, Omsk State Technical University, Russia, Omsk
Mikhailov Sergey Yurievich
Student, Radio Engineering Faculty, Omsk State Technical University, Russia, Omsk

УДК 004.032

ШТАТНЫЕ МЕХАНИЗМЫ ЗАЩИТЫ ИНФОРМАЦИИ И ЖУРНАЛИРОВАНИЯ СОБЫТИЙ БЕЗОПАСНОСТИ В ОС WINDOWS

STAFF MECHANISMS OF INFORMATION PROTECTION AND JOURNALIZATION OF WINDOWS SECURITY EVENTS

Аннотация: в ходе данной статьи рассмотрены в теории и реализованы на практике штатные механизмы защиты информации и журналирования событий безопасности в ОС Windows.

Abstract: during this article, we reviewed in theory and implemented in practice the regular mechanisms for protecting information and logging security events in Windows OS.

Ключевые слова: операционная система, безопасность, программное обеспечение, события безопасности, журналирование, аудит.

Keywords: operating system, security, software, security events, logging, auditing.

Для обеспечения защиты информации, содержащейся в информационной системе, оператором назначается структурное подразделение или должностное лицо (работник), ответственные за защиту информации.

Защита информации, содержащейся в информационной системе, является составной частью работ по созданию и эксплуатации и вывода из эксплуатации путем принятия организационных и технических мер защиты информации, направленных на блокирование угроз безопасности информации в информационной системе, в рамках системы защиты информации информационной системы .

Информация, содержащаяся в информационной системе, подлежит следующей системе мероприятий:

- формирование требований к защите информации, содержащейся в информационной системе;
- разработка системы защиты информации информационной системы;
- внедрение системы защиты информации информационной системы;
- аттестация информационной системы по требованиям защиты информации и ввод ее в действие;
- обеспечение защиты в ходе эксплуатации аттестованной информационной системы;

- обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.

Формирование требований к защите информации, содержащейся в информационной системе, осуществляется обладателем информации. Организационные и технические меры защиты информации, реализуемые в информационной системе в рамках ее системы защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационной системы должна обеспечивать:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам;
- ограничение программной среды;
- защиту машинных носителей информации;
- регистрацию событий безопасности;
- антивирусную защиту;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- доступность информации;
- защиту среды виртуализации;
- защиту технических средств;
- защиту технических средств;
- защиту информационной системы, ее средств, систем связи и передачи данных.

Класс защищенности информационной системы определяется в зависимости от уровня значимости информации, обрабатываемой в этой информационной системе, и масштаба информационной системы.

Уровень значимости информации определяется степенью возможного ущерба для обладателя информации и (или) оператора от нарушения конфиденциальности, целостности или доступности информации.

Класс защищенности информационной системы определяется в соответствии с таблицей 1:

Таблица 1

Определение класса защищенности

Уровень защищенности информации	**Масштб информационной системы**		
	федеральный	**региональный**	**объектовый**
УЗ 1	К1	К1	К1
УЗ 2	К1	К2	К2
УЗ 3	К2	К3	К3

Меры защиты информации для данной информационной системы

В таблице 2 приведены сокращения наименований, а также их пояснения.

Таблица 2

Наименования и их сокращения

Сокращение	**Расшифровка**
ИАФ	Идентификация и аутентификация субъектов и объектов доступа
УПД	Меры управления доступом
ГИС	Государственная информационная система
ОПС	Ограничение программной среды
РСБ	Регистрация событий безопасности

- **ИАФ 1** – идентификация и аутентификация пользователей, являющихся работниками оператора.
- **ИАФ 5** – защита обратной связи при вводе аутентификацион. информации.
- **УПД 2** – реализация необходимых и методов (дискреционный, мандатный, ролевой или иной метод), типов и правил (чтение, запись, выполнение или иной тип) разграничения доступа.
- **ОПС 2** – управление установкой (инсталляцией) компонентов программного обеспечения.
- **РСБ 2** – определение состава и содержания информации о событиях безопасности, подлежащих регистрации.

В таблице 3 приведена матрица разграничения доступа объктов информационной системы к соответствующим субъектам. По данным сведениям будет производиться настройка УПД в практической части работы.

Таблица 3
Матрица доступа

	Docs/U1	**Docs/U2**	**distr**	**Docs/K1**	**Docs/K2**
Adm-1	*R W CR D*	*R W CR D*	*R W CR D*	*R W CR D*	*R W CR D*
Adm 2	*R W CR D*	*R W CR D*	*R W CR D*	*R W CR D*	*R W CR D*
Usr-1	*R W CR D*	-	-	*W R*	*R*
Usr-2	-	*R W CR D*	-	-	*WR*
System	*R W CR D*	*R W CR D*	*R W CR D*	*R W CR D*	*R W CR D*

В ходе данной работы все нижеописанные действия будут производиться на виртуальной машине с ОС *Windows 7*.

Исходя из таблицы 3, рассматриваемый АРМ содержит в себе 4 учетных записи (пользователей), а именно 2-х администраторов (*sa-1, sa-2*) и 2-х пользователей (*usr-1, usr-2*). Прежде всего необходимо создать и настроить данные учетные записи:

Панель управления – Учетные записи пользователей и семейный доступ – Добавление и удаление учетных записей пользователей.

На рисунке 1 показан результат создания и настройки учетных записей.

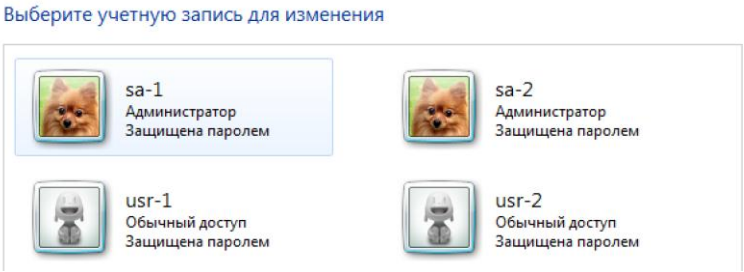


Рис. 1. Учетные записи пользователей

На диске С создадим директории, взятые из таблицы 3, а именно *«docs/usr-1», «docs/usr-2», «distr», «docs/Конфи1», «docs/Конфи2»*. После создания настроим меры управления доступом, то есть реализуем составленную в теоретической части матрицу доступа. Для этого необходимо зайти под администратором, выбрать соответствующую директорию, кликнуть правой кнопкой мыши и нажать на «Свойства». В появившемся окне перейти на вкладку «Безопасность» (рисунок 2).

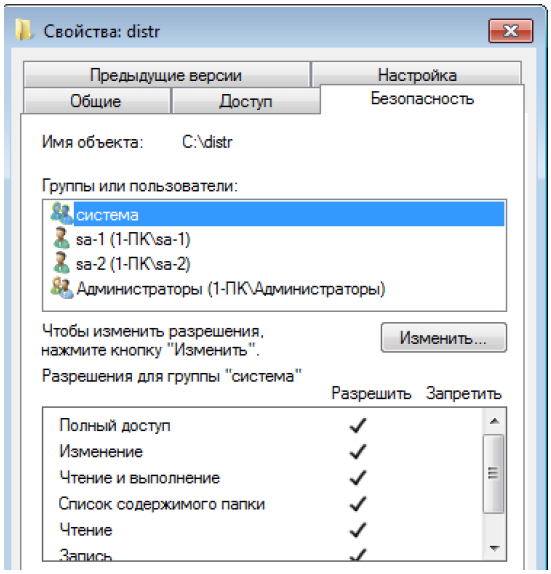


Рис. 2. Настройка УПД

После настройки проверим ее корректность. Для этого выберем, например, пользователя «*usr-1*» и попытаемся получить доступ к директории «*distr*». Согласно таблице 3 рассматриваемый пользователь не имеет доступа к данной директории. На рисунке 3 отображено реагирование системы, а именно ограничение доступа, что свидетельствует о правильной настройке мер управления доступом.

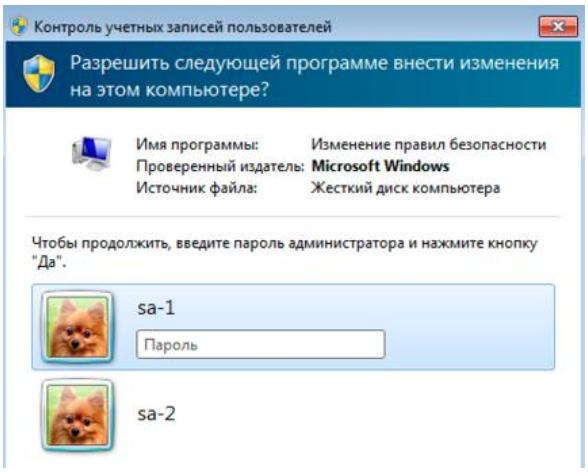


Рис. 3. Ограничение системы (УПД)

Следующим шагом в настройке АРМа является ограничение программной среды, а именно тот факт, что пользователи, которые не являются администраторами системы, не имеют возможности устанавливать компоненты программного обеспечения, запуска исполняемых файлов. Для этого перейдем по пути:

Панель управления – Учетные записи пользователей и семейная безопасность – Родительский контроль – Средства управления пользователем.

В открывшемся окне выберем ссылку «*Разрешение и блокировка конкретных программ*» (рисунок 4), после чего откроется новое окно, в котором необходимо выбрать программное обеспечение, разрешенное для запуска для соответствующего пользователя.

Рис. 4. Настройка ОПС

Проверим корректность настройки ограничения программной среды. Для этого войдем в систему под настраиваемым пользователем и запустим программу, которая не является разрешенной, например, «*GoogleChrome*». Результат отображен на рисунке 5, что свидетельствует о правильной настройке.

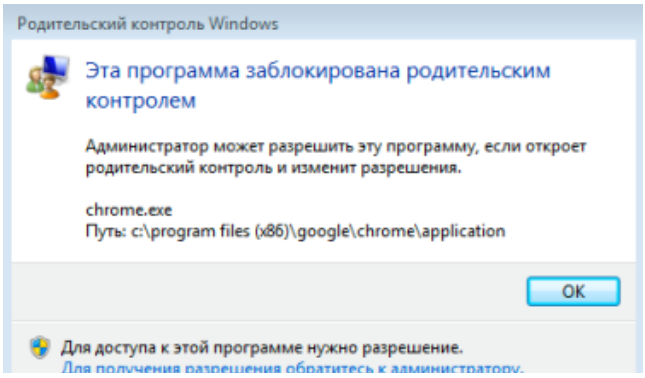


Рис. 5. Ограничение системы (ОПС)

Следующий шаг заключается в настройке регистрации событий безопасности. Например, когда пользователь «usr-1» обращается в директорию «distr», в журнал безопасности Windows прописывается данное действие. Перейдем по следующему пути:

Панель управления – Система и безопасность – Администрирование – Локальная политика безопасности.

В открывшемся окне выберем вкладку «*Локальные политики – Политика аудита*» (рисунок 6), после чего произведем конфигурацию.

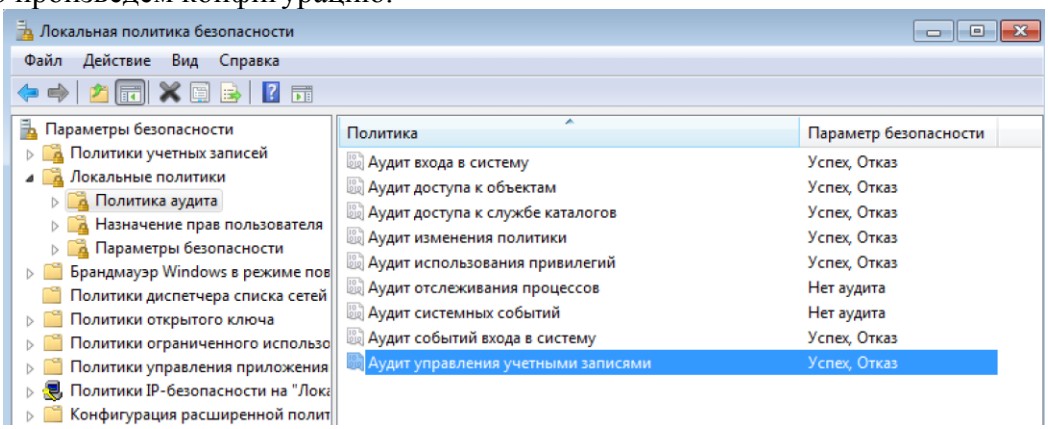


Рис. 6. Настройка политик аудита

После этого перейдем к защищаемым директориям, кликнем правой кнопкой мыши, выберем раздел «*Свойства*». В открывшемся окне переходим по вкладке «*Безопасность*», жмем на «*Дополнительно – Аудит*». В результате перед пользователем появится форма, в которой необходимо настроить правила аудита (рисунок 7, 8).

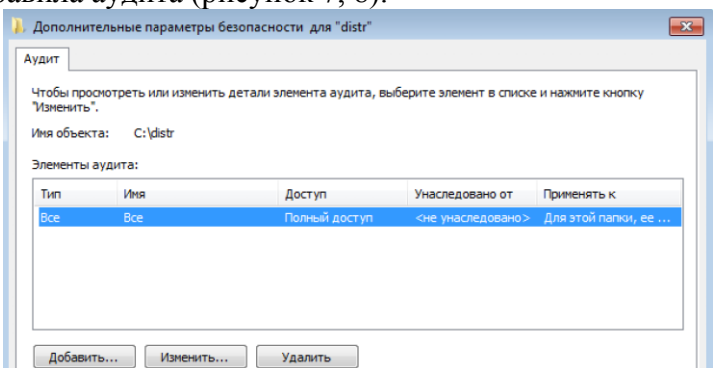


Рис. 7. Настройка аудита

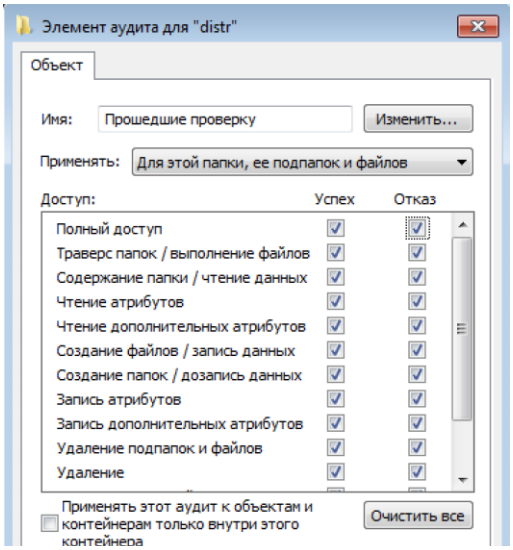


Рис. 8. Элемент аудита

После вышеописанных действий любое обращение к защищаемым директориям будет прописываться в журнал событий Windows в графе «*Безопасность*». Так, например, на рисунке 9 представлен аудит успеха пользователя «*sa-1*» в директорию «*distr*».

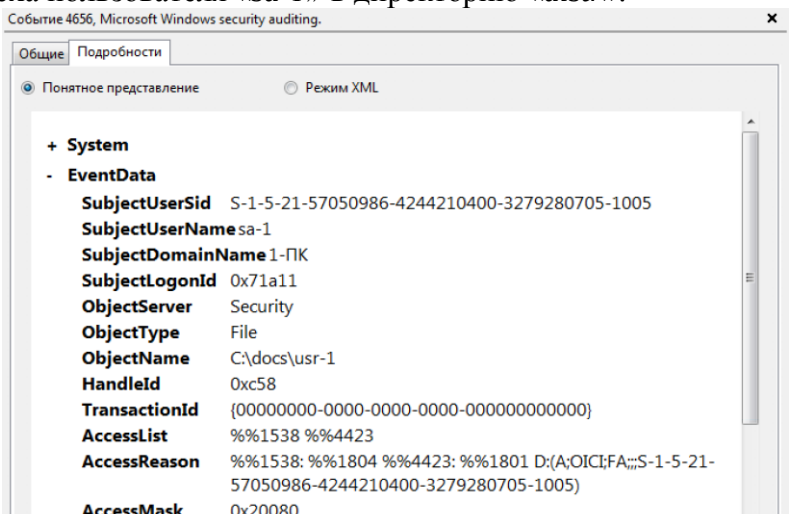


Рис. 9. Аудит успеха УПД

Также бывает целесообразно опередить максимальный размер журнала событий Windows. Для этого необходимо выбрать соответствующий журнал, после чего нажать на правую кнопку мыши и выбрать раздел «Свойства». В появившемся окне произвести настройку (рисунок 10).

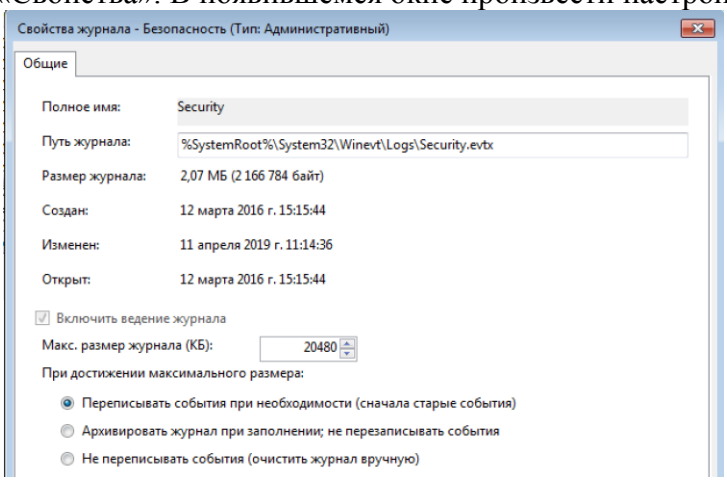


Рис. 10. Настройка журнала событий

Таким образом, в ходе данной работы рассмотрены в теории и реализованы на практике штатные механизмы защиты информации и журналирования событий безопасности в ОС Windows.

Библиографический список:

1. Конявский, В. А., Гадасин В. А. Основы понимания фе- номена электронного обмена информацией (Библиотека жур-нала "УЗИ"; Кн. 2). — Мн.: "Беллитфонд", 2004. — 282 с.

2. "Доверенная гарвардская" архитектура – компьютер с динамически изменяемой архитектурой / Комплексная защита информации: материалы XX науч.-практ. конф., Минск, 19– 21 мая 2015 г. — Мн.: РИВШ, 2015. С. 32—37.

3. Конявский В. А. Доверенный сеанс связи. Развитие парадигмы доверенных вычислительных систем — на старт, внимание, МАРШ! / Комплексная защита информации. Материалы XV межд. науч.-практ. конф., Иркутск, 1–4 июня 2010 г. — М., 2010.

4. Каннер А. М. Средство организации доверенного сеанса как альтернатива доверенной вычислительной среде // Ин- формационные технологии управления в социально- экономических системах. — М., 2010. Вып. 4. С. 140—143.

5. Счастный Д. Ю. Ноутбук руководителя / Комплексная защита информации: материалы XX науч.-практ. конф., Минск, 19–21 мая 2015 г. — Мн.: РИВШ, 2015. С. 112, 113.

Коллектив авторов

Сборник материалов XLIII Международной научной конференции «Техноконгресс»

ISBN 978-5-9907998-1-3

Техниконаучный журнал «Техноконгресс»

Кемерово 2019