

# Дмитрий Андриянков

## Местоположение

Проживание: Россия, Москва

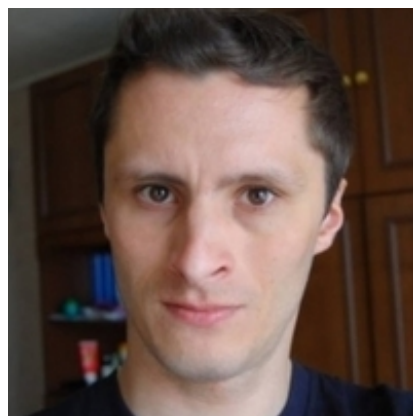
## Возраст и стаж

Стаж: 13 лет и 9 месяцев

Возраст: 37 лет

## Контактная информация

Мой круг: <https://moikrug.ru/andriyankov>



---

## Профессиональные навыки

---

Системное программирование • Обратная разработка • Тестирование ПО • Разработка через тестирование • Python

---

## Опыт работы

---

Октябрь 2010 –  
По наст. время  
(8 лет и 8 месяцев)

### Passware (Lostpassword.com)

Тестировщик  
Россия, Москва

#### Обязанности и достижения

Обязанности: - Тестирование существующих и новых возможностей продуктов - Планирование процесса тестирования продукта. Организация тестовых сценариев и их наборов - Разработка нового и поддержка существующего кода Достижения: - Принял участие в разработке "<http://www.lostpassword.com/encase.htm>" - Продукт стал лучше в результате исправления найденных мною багов

Июль 2010 –  
Октябрь 2010  
(4 месяца)

### ЗАО "АСТ"

Windows Программист  
Россия, Москва

#### Обязанности и достижения

Обязанности: - Разработка и отладка нового системного кода В данной должности активно применял WinDbg, IDA Pro, Hiew, MS Visual Studio 2008/2010 Team и Express варианты. А также TortoiseSVN

Июль 2008 –  
Апрель 2010  
(1 год и 10 месяцев)

### Лаборатория Касперского

Вирусный аналитик  
Россия, Москва

#### Обязанности и достижения

Обязанности: - Разработка системного кода: статических распаковщиков и кодоанализаторов, детектирующих полиморфные объекты - Анализ файлов, как правило исполнимых, для выявления вредоносной составляющей и вынесение вердикта о безопасности файла Достижения: - Написаны статические распаковщики к продуктам - Написаны детектирующие кодоанализаторы полиморфных

объектов Значительно улучшил навыки использования: • Hiew, IDA Pro, VB Decompiler; • OllyDebugger; • Sysinternals ProcessMonitor, ProcessExplorer, Autoruns и др.; • MS Debugging tools(WinDBG в частности); • O10 Editor;

Декабрь 2007 –  
Июнь 2008  
(7 месяцев)

## **Научно-Исследовательский Центр CALS-технологий** **Прикладная логистика**

Программист Delphi

Россия, Москва

### **Обязанности и достижения**

Обязанности: - Разработка нового и сопровождение существующего кода для автоматизированной системы предназначенной для использования инженерами-конструкторами авиационной промышленности

Июль 2005 –  
Ноябрь 2007  
(2 года и 5 месяцев)

## **Филиал "ТАТЭНЕРГО" ОАО "Нижнекамская ТЭЦ"**

Инженер-программист

Россия, Нижнекамск

### **Обязанности и достижения**

\*Должностные обязанности:\* Поддержание работоспособности и модернизация для повышения отказоустойчивости систем АСУТП на Нк ТЭЦ; \*Функции:\* • Разработка нового ПО для систем АСУТП нижнего уровня на Нк ТЭЦ; • Сопровождение существующего ПО как высокого, так и нижнего уровней систем АСУТП на Нк ТЭЦ; • Документирование существующих и вновь внедряемых продуктов; \*Достижения:\* • Модернизация старой системы АИС Контроля и Учета Тепла на Нк ТЭЦ, путем внедрения новой и значительно улучшенной версии мною разработанного приложения нижнего уровня на Delphi 2007 for Win32 ; • Модернизация старой системы сбора данных по протеканию технологического процесса, путем разработки ПО нижнего уровня на BDS 2006 Enterprise. Данное ПО реализует и инкапсулирует следующие задачи: - Производит опрос OPC-серверов от различных SCADA-систем и различных производителей; - Реплицирует полученные данные в файлы местного формата; - Реплицирует в базу данных под управлением СУБД Oracle; - Предоставляет данные через сеть клиентским АРМам; • Модернизация старой системы учета потребляемого Нк ТЭЦ азота, путем внедрения разработанного мною ПО на Delphi 7; • Исправил сложную программную ошибку в ПО высокого уровня системы АСУТП, разработанного программистом до моего трудоустройства на Нк ТЭЦ; • Автоматизировал процесс очищения временных файлов на ЭВМ пользователей, после системы "Парус" и Crystal Reports, что позволило снизить дефекты в системе документо-оборота на предприятии;

---

## **Высшее образование**

---

Январь 2000 –  
Январь 2006

## **Казанский национальный исследовательский технический университет (бывший КГТУ) им. А. Н. Туполева**

Технической кибернетики и информатики

Россия, Казань

### **Специализация и достижения**

Защитил на "Отлично" дипломный проект: "АИС контроля и учета

## О себе

---

Специализация и профессиональные навыки:

\*Специализация:\*

- Исследование работы исполняемых файлов;
- Разработка программ по взлому защищенных программ(PE/PE32+);
- Разработка кодоанализаторов обфусцированных исп. объектов для обнаружения или выделения функциональности

\*Языки программирования:\*

- C\C++(STL, Boost, Google.Test) - непрерывно улучшаю навыки по ним;
- Ассемблер(x86-64 код) - небольшие стабы\вставки и чтение кода;
- Python - скрипты для автоматизации рутинных действий.

\*Средства разработки:\*

- MS Visual Studio 2013.
- Python 3.x пишу в Sublime Text;
- Flatassembler;
- Perforce, SVN, Mercurial, Git.

Профессиональные цели:

Стремлюсь работать в проектах направленных на создание и развитие продуктов улучшающих жизнь человека

Награды, сертификаты, портфолио, проекты:

\*Мои блоги и статьи:\*

<http://ntvisigoth.blogspot.com/> - посвящен теме reversing-engineering;

<http://nobunkum.ru/ru/static-analysis> - Некоторые приёмы статического анализа кода из арсенала вирусного аналитика;

<http://wasm.ru/print.php?article=gost29147-89> - Алгоритм шифрования ГОСТ 28147-89. Метод простой замены.

[http://habrahabr.ru/blogs/system\\_programming/129241/](http://habrahabr.ru/blogs/system_programming/129241/) - Разработка функций RvaToRaw и RawToRva

Дополнительная информация:

- Учусь быть хорошим отцом(дочурка это круто);
- Люблю свою работу(Хотя порою Agile иногда выбешивает, но он не реально полезный);
- Работал, работаю и буду стремиться дальше работать с серьезными спецами в своем деле;
- Стремлюсь работать там, где душе комфортно.

В данный момент пишу свой небольшой research-инструмент для анализа с исполняемых файлов PE32\PE32+ с тем функционалом в котором нуждаюсь сам и мои знакомые реверсеры.