

НЕГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ ЧАСТНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ФИНАНСОВО-ПРОМЫШЛЕННЫЙ УНИВЕРСИТЕТ «СИНЕРГИЯ»
Колледж «Синергия»
Департамент цифровой экономики

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА – ДИПЛОМНЫЙ ПРОЕКТ

НА ТЕМУ: ВНЕДРЕНИЕ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ООО
«АСТРА»

Специальность **09.02.04** Информационные системы (по отраслям)

ФИО обучающегося: Рогожников Егор Дмитриевич
Группа: ОБИ-3809МО
ФИО Руководителя: Терехова Лидия Анатольевна



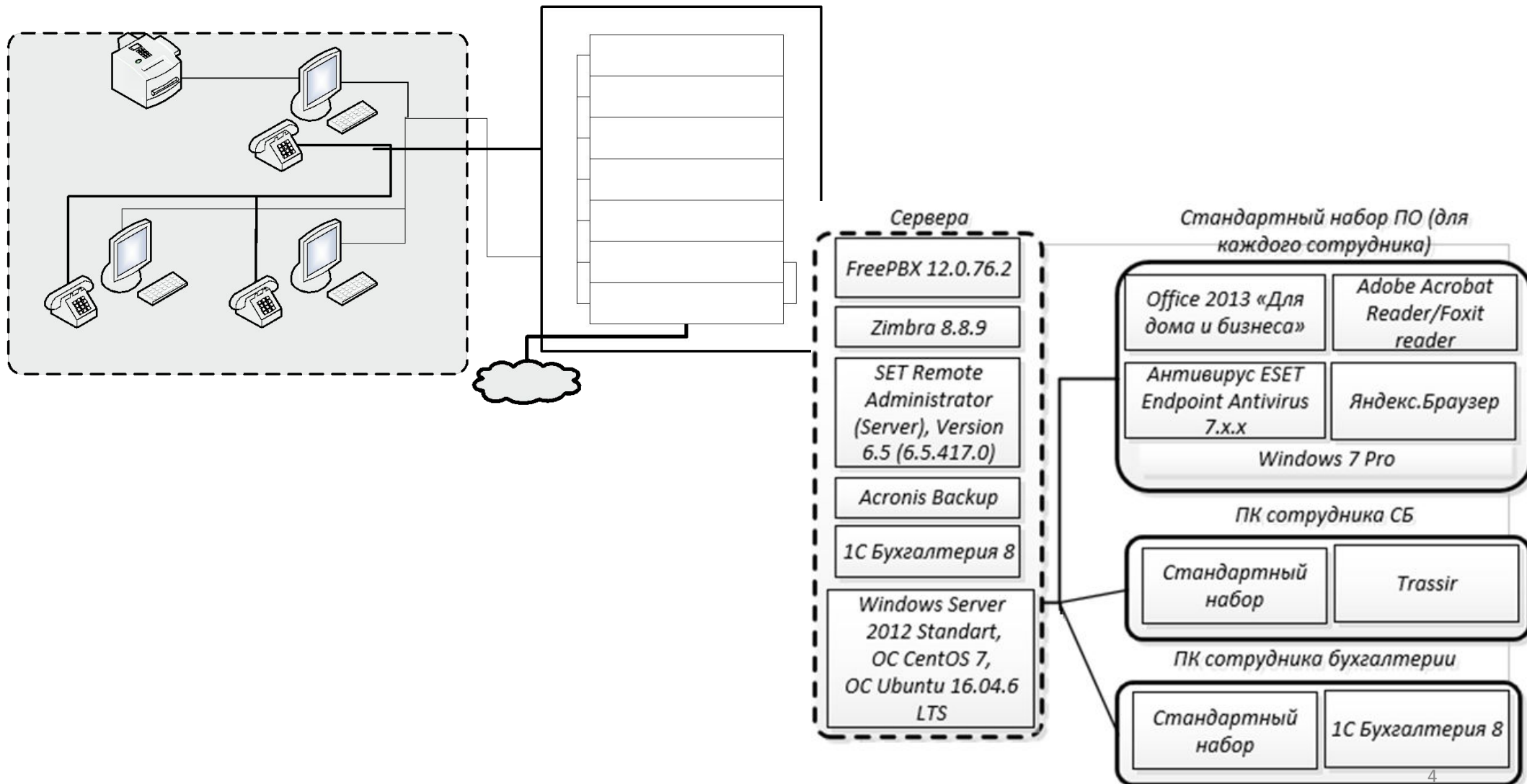
Цель и задачи работы:

- В качестве объекта исследования в моей работе выступает предприятие ООО "Астра", в качестве предмета исследования рассматривается процесс по разработке организационно-технических решений, связанных с обеспечением защиты информации на рабочих местах в корпоративной сети предприятия.
- Целью предоставленной работы считается внедрение комплексной защиты информации в ООО "Астра".
- Для достижения заданной цели необходимо выполнить ряд задач:
 - - провести техническую и экономическую характеристику предметной области рассматриваемого предприятия;
 - - провести моделирование предметной области, дать характеристику комплексу задач, задаче и обоснованию необходимости в усовершенствовании системы обеспечения ИБ и защите информации на рассматриваемом предприятии;
 - - произвести обзор антивирусов и выбрать стратегию автоматизации;
 - - провести инфологическое и программное проектирование предметной области;
 - - обосновать экономическую эффективность разработанного проекта.

Методы исследования

- Для выполнения назначенных задач использовались теоретические и эмпирические методы исследования.
- Методы исследования:
 - анализ деятельности предприятия и выявления области автоматизации;
 - анализ теоретических источников по проблеме исследования;
 - объектно-ориентированное моделирование при разработке программного продукта;
 - функциональное моделирование при разработке диаграмм IDEF0.
- При написании проекта применялись такие способы научного исследования: изучение нормативно-правовой базы, научной литературы по теме исследования, сравнительный и аналитический способы.

Техническая и программная архитектура предприятия



Выбор средств реализации

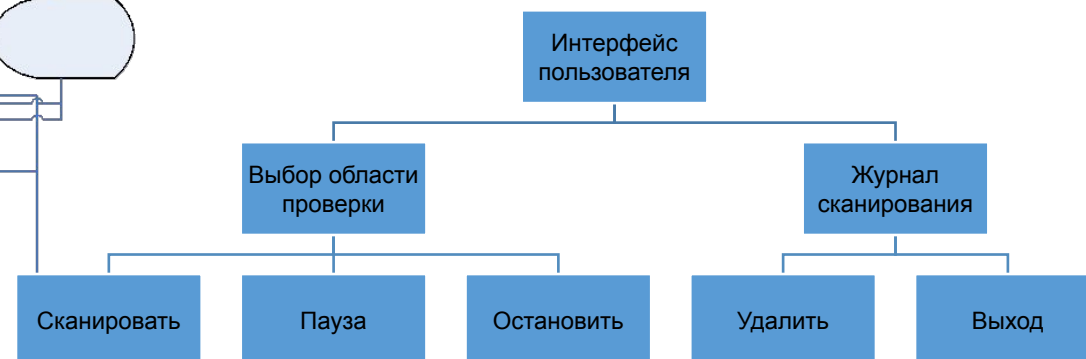
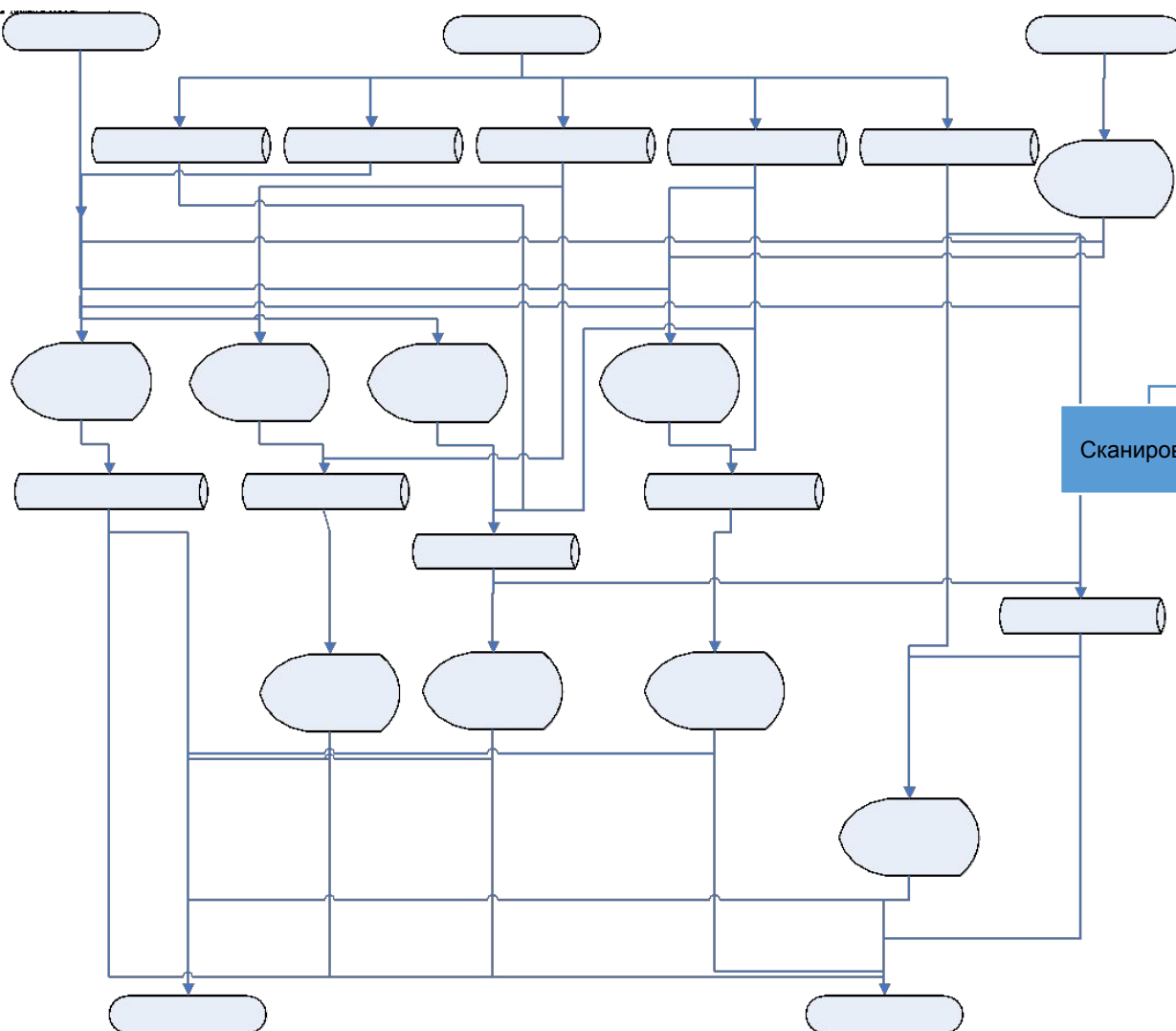
Language Rank	Types	Spectrum Ranking
1. Python		100.0
2. C++		99.7
3. Java		97.5
4. C		96.7
5. C#		89.4
6. PHP		84.9
7. R		82.9
8. JavaScript		82.6
9. Go		76.4
10. Assembly		74.1

Популярность языков программирования в 2020 году

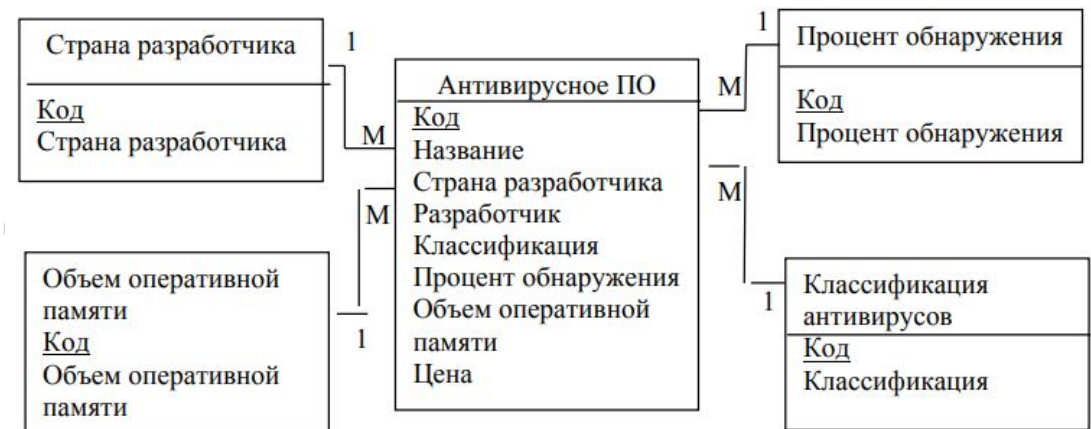
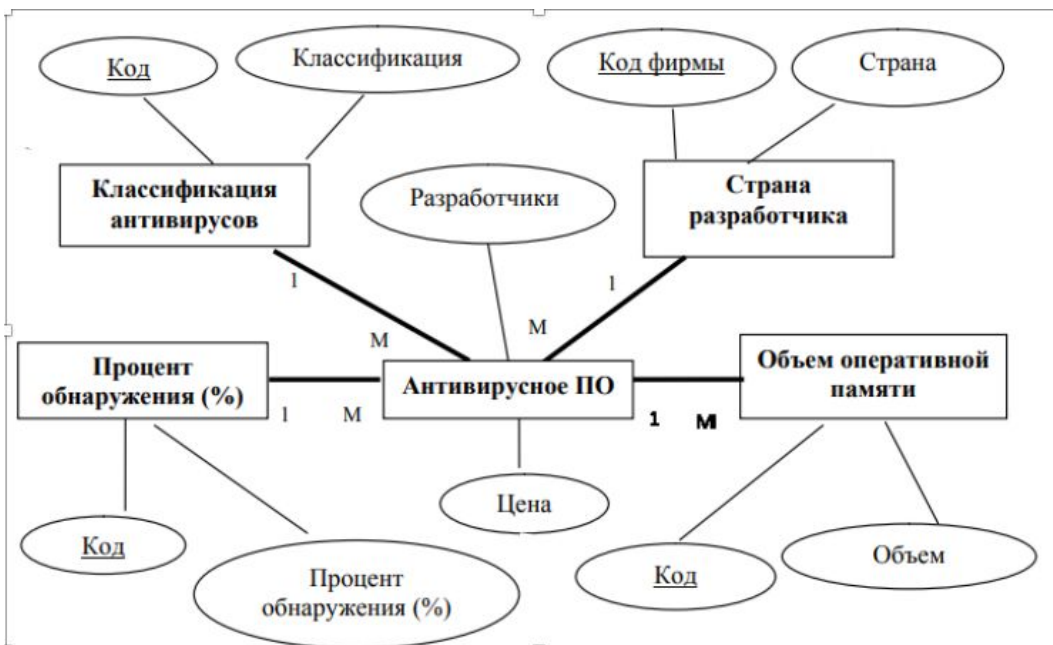
Критерии\ Языки	C#	Python	C++	Java	C	R	Go
Простота реализации программы	5	4	4	3	5	4	4
Кроссплатформенность	4	4	5	5	4	5	3
Гибкость	5	4	4	3	3	4	4
Цена	5	5	5	4	4	3	5
Безопасность	5	4	4	4	5	5	4
Интеграция	5	3	4	3	4	4	3
Открытость исходного кода	5	4	4	5	5	4	4
Универсальность приложений	4	5	5	5	3	4	3
Общая оценка	38	33	31	32	33	33	30

	Visual Studio	Project Rider	Eclipse	Visual Studio Code	MonoDevelop	Code::Blocks
Преимущества	<ul style="list-style-type: none"> - Официальная. - Бесплатная. - Функциональная. - Поддерживает платформы .NET. - Облачные хранилища. - Корпоративность. 	<ul style="list-style-type: none"> - ReSharper. - Поддержка полного цикла. - Функциональность. - Multiple runtime. - Кроссплатформенность. - Контроль версий. 	<ul style="list-style-type: none"> - Множество плагинов. - Активное сообщество. - Отличные компилятор и отладчик. - Кастомизация. - Бесплатность. - Высокая функциональность. 	<ul style="list-style-type: none"> - Кроссплатформенность. - Бесплатность. - Легковесность.. 	<ul style="list-style-type: none"> - Мультиплатформенность. - Кастомизация. - Unity 3D. - Бесплатность. 	<ul style="list-style-type: none"> - Бесплатность. - Простота. - Кроссплатформенность. - Выбор компилятора. - Легковесность.
Недостатки	<ul style="list-style-type: none"> - Баги при переходах с триал-версии. - Сложность. 	<ul style="list-style-type: none"> - Молодость. - Стоимость. 	<ul style="list-style-type: none"> - Сложность. - Нет гарантий надежности. 	<ul style="list-style-type: none"> - Низкая функциональность. - Сомнительная надежность. 	<ul style="list-style-type: none"> - Ограниченная функциональность. 	<ul style="list-style-type: none"> - Недостаточная функциональность.

Информационная модель и Структурная схема программы



ER-диаграмма и Логическая модель БД



Результаты работы ПО

56 engines detected this file

SHA-256: efc94fdac8753451e7070f0cccb1b8e2ba2ce9e6edd3378a7ac412a359a256e4
 File name: malware.exe
 File size: 20 KB
 Last analysis: 2018-05-08 17:52:00 UTC
 Community score: -45

AhnLab-V3	✓ Clean	Avast Mobile Security	✓ Clean
Babable	✓ Clean	CMC	✓ Clean
eGambit	✓ Clean	Endgame	✓ Clean
Kingsoft	✓ Clean	Malwarebytes	✓ Clean
Sophos ML	✓ Clean	SUPERAntiSpyware	✓ Clean
Zoner	✓ Clean	Alibaba	Unable to process file type
CMC	✓ Clean	Comodo	✓ Clean
Cyren	✓ Clean	DrWeb	✓ Clean
eGambit	✓ Clean	F-Prot	✓ Clean
Fortinet	✓ Clean	Ikarus	✓ Clean
Jiangmin	✓ Clean	Kingsoft	✓ Clean
McAfee	✓ Clean	Microsoft	✓ Clean

31 engines detected this file

SHA-256: 4be0a30ebfb7000a9bb3c4a7308870375fcbf4e4122c6cb57dd1aa53c79184a3
 File name: 2.exe
 File size: 15.41 KB
 Last analysis: 2018-06-05 15:38:36 UTC

Palo Alto Networks	✓ Clean	Panda	✓ Clean
Rising	✓ Clean	Sophos AV	✓ Clean
SUPERAntiSpyware	✓ Clean	TACHYON	✓ Clean
Tencent	✓ Clean	TheHacker	✓ Clean
VIPRE	✓ Clean	ViRobot	✓ Clean
Webroot	✓ Clean	Yandex	✓ Clean
Zillya	✓ Clean	ZoneAlarm	✓ Clean
Zoner	✓ Clean	Alibaba	Unable to process file type
Symantec Mobile Insight	Unable to process file type	Trustlook	Unable to process file type

Сравнительные результаты анализа УНИВЕРСИТЕТ СИНЕРГИЯ упакованных, обфусцированных и модифицированных образцов ВПО

Образец ВПО	Характеристики до модификации (размер/энтропия)	Характеристики после модификации (размер/энтропия)	Результат анализа (АС не справившиеся с модификацией)
1	20KB 6.3206	15.41KB 7.4055	37.3%
2	263KB 4.1235	105.91KB 7.9599	30.3-32.3%
3	418.13KB 6.2405	39.92 KB 7.3060	58.2%

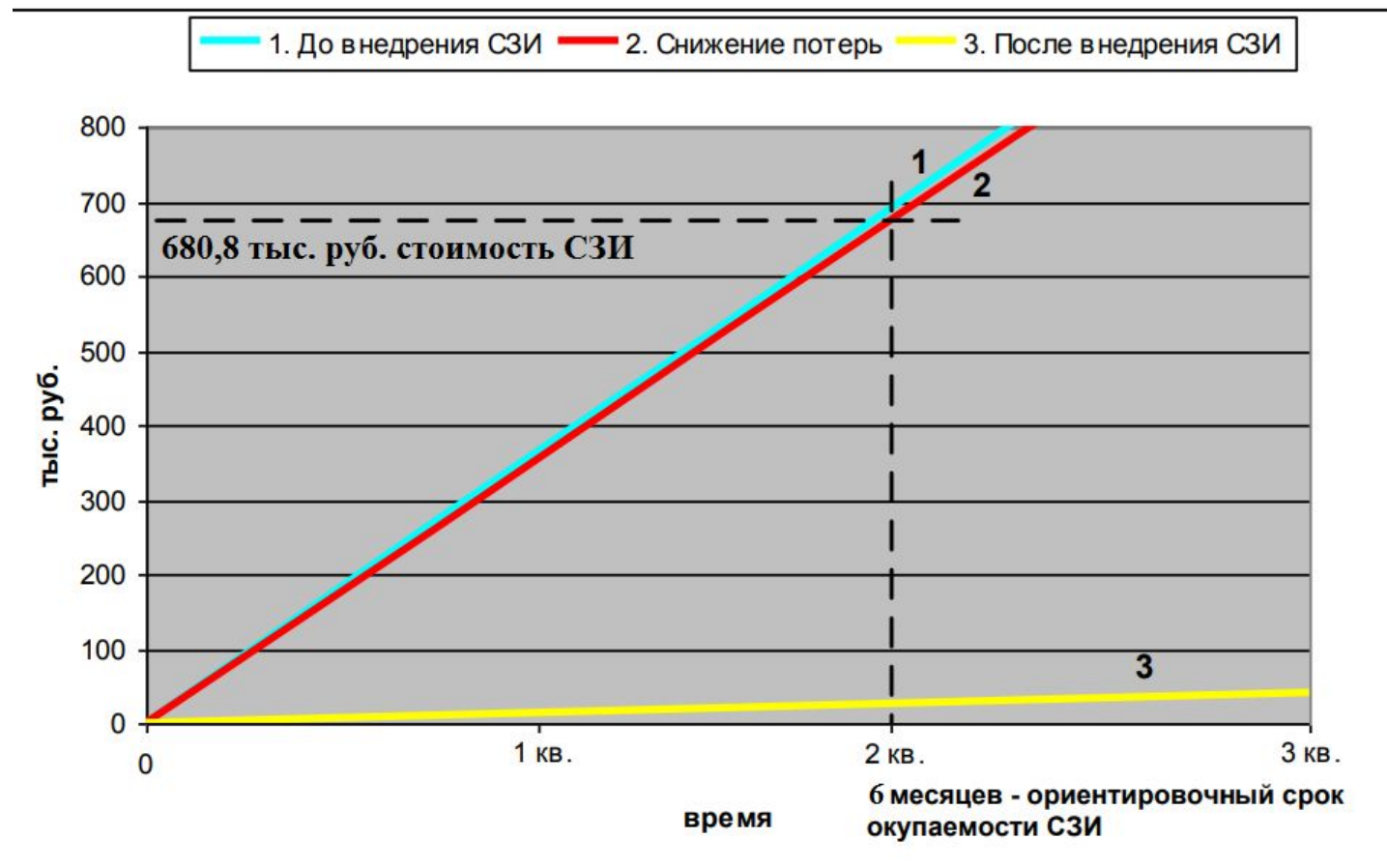
Образец ВПО	Характеристики до модификации (вес/энтропия)	Характеристики после модификации (вес/энтропия)	Результат анализа (АС не справившиеся с модификацией)
1	20KB 6.3206	1.83MB 6.1197	40.3%
2	263KB 4.1235	2.04MB 6.2950	30.3-32.3%
3	418.13KB 6.2405	2.24MB 6.1822	46.3%

Образец ВПО	Характеристики до модификации (вес/энтропия)	Характеристики после модификации (вес/энтропия)	Результат анализа (АС не справившиеся с модификацией)
1	20KB 6.3206	1.02MB 7.8239	41.8%
2	263KB 4.1235	1.1MB 7.8446	44.8%
3	418.13KB 6.2405	1.06MB 7.8018	46.3%

Выводы

- Результатом проведённой работы стало создание программы-упаковщика, с помощью которой были произведены модификации нескольких образцов ВПО с целью тестирования работоспособности АС.
- В ходе работы стало известно, что в современных условиях необходимо своевременное обнаружение ВПО и применение комплексных мер, направленных на предотвращение последствий их работы. Именно этим и занимаются антивирусное ПО.
- Изучив состояние вопроса на данный момент, становится очевидным необходимость создания ПО для анализа уязвимостей АС. Примером такого ПО является разработанный в данной работе упаковщик. Принцип и результаты работы разработанной программы наглядно и подробно продемонстрированы.
- Работа с информационной системой происходит в диалоговом режиме, который предоставляет пользователю возможность взаимодействовать с хранящейся в системе информацией в режиме реального времени, получая при этом всю необходимую информацию для решения функциональных задач.
- Разработанная программа имеет удобный пользовательский интерфейс. При запуске программы открывается форма авторизации, поскольку права пользователей для работы с системой разграничены. При успешной авторизации открывается форма «Главная», в которой можно выбрать пункты меню или кнопки для работы с формой.

Результаты экономической эффективности внедрения ПО



$$T_{ок} = R \sum / (R_{ср} - R_{прогн})$$

$$T_{ок} = 680,800 / (1,430,000 - 66,800)$$

$$T_{ок} = 0,5$$

СПАСИБО ЗА ВНИМАНИЕ!

БОЛЬШЕ ЧЕМ
ОБРАЗОВАНИЕ

1988