**Федеральное государственное образовательное бюджетное**

**учреждение высшего образования**

**«Финансовый университет при Правительстве Российской Федерации»**

**(Финансовый университет)**

Факультет Информационных технологий и анализа больших данных

Департамент/Кафедра Информационная безопасность

**ОТЧЕТ**

по производственной, в том числе преддипломной практике (производственная практика: проекто-технологическая практика, преддипломная практика)

*(указать вид (тип/типы) практики)*

Направление подготовки/Специальность «Информационная безопасность»

*(наименование направления подготовки/специальности)*

Безопасность автоматизированных систем в финансово-банковской сфере

*(профиль образовательной программы бакалавриата/направленность образовательной программы магистратуры/направленность образовательной программы специалитета)*

Выполнил:

Обучающийся учебной группы: \_ ИБ19-2

Д.Е. Ростовский

*(подпись) (И.О. Фамилия)*

Проверили:

Руководитель практики от организации:

Директор Дирекции развития и

сопровождения банковских платформ С.Н. Симоненко

*(должность) (И.О. Фамилия)*

*(подпись)*

М.П.

Руководитель практики от департамента/кафедры:

к.х.н., доцент С.П. Капинос

*(ученая степень и/или звание) (И.О. Фамилия)*

*(оценка) (подпись)*

**Москва – 2023**

Содержание

[1. MaxPatrol 8 3](#_Toc134103655)

[1.1. Установка MaxPatrol 8 3](#_Toc134103656)

[1.2. Создание задач сканирования 4](#_Toc134103657)

[2. Метрики оценивания опасности обнаруженных уязвимостей 5](#_Toc134103658)

[2.1. Общая система оценки уязвимостей (CVSS) 5](#_Toc134103659)

[2.2. Метрики CVSS 5](#_Toc134103660)

[3. Список регулярных уязвимостей большинства современных информационных систем 7](#_Toc134103661)

[3.1. OWASP Top 10 7](#_Toc134103662)

[3.2. Positive technologies vulnerabilities database 7](#_Toc134103663)

[Заключение 9](#_Toc134103664)

[Список использованных источников 10](#_Toc134103665)

# Технико-экономическое обоснование разработки программного решения по мониторингу активных информационных сервисов

# Техническое задание по проекту

Составлено техническое задание (ТЗ) на внедрение автоматизированной информационной системы (АИС), позволяющей работать с электронной подписью. Техническое задание составлено в соответствии с ГОСТ 34.602-89.

1. Введение

Настоящее техническое задание распространяется на разработку АИС «Система мониторинга», используемой для хранения и передачи данных, используемых всеми пользователями АИС, в соответствии с уровнем доступа.

2. Основание для разработки

Программное обеспечение АИС «Система мониторинга» разрабатывается на основании «Требований к автоматизированной системе организации», в соответствии с заданием, полученным у отдела безопасности.

3. Назначение разработки

3.1. Назначение

Основное назначение АИС «Система мониторинга» заключается в оптимизации и улучшения безопасности электронного документооборота сотрудников организации.

3.2. Исходные данные

Исходными данными для разработки являются требования налогового кодекса Российской Федерации (НК РФ), требования владельца и требования иных нормативно-правовых документов организации.

3.3. Цель работы

Целью работы является создание прототипа АИС «Система мониторинга» для обеспечения безопасного электронного документооборота.

3.4. Решаемые задачи

* Математическая постановка основных задач и выбор методов решения этих задач.
* Определение архитектуры АИС: разработка её структуры; определение набора необходимого оборудования, программного обеспечения и процессов обслуживания.
* Анализ требований технического задания и разработка спецификаций проектируемой АИС.
* Реализация компонентов с использованием выбранных средств и их автономное тестирование.
* Сборка АИС «Система мониторинга» и её комплексное тестирование.
* Оценочное тестирование удобства использования, стабильности АИС и её защищённости.

4. Требования к АИС

4.1. Требования к функциональным характеристикам

АИС «Система мониторинга» должна обеспечивать возможность выполнения перечисленных ниже функций:

- автономный процесс сбора данных

- работа по систематизации данных

Исходные данные:

- несистематизированные данные

Результаты:

- систематизированные данные

4.2. Требования к надёжности

Надёжное (устойчивое) функционирование АИС должно быть обеспечено выполнением Заказчиком совокупности организационно-технических мероприятий, перечень которых приведён ниже:

- оказание консультаций по вопросам работы сети;

- восстановление работоспособности сети передачи данных и оказание услуг связи до границы ответственности Исполнителя;

- настройка конфигурации оборудования согласно рекомендациям заказчика.

4.3. Условия эксплуатации

4.3.1 Условия эксплуатации в соответствие с СанПин 2.2.2.542 – 96.

4.3.2 Обслуживание обеспечивается персоналом исполнителя или иными организациями, аттестованными для работы с АИС

4.3.3 Обслуживающий персонал может оптимизировать систему, обновлять её компоненты и восстанавливать частично утраченную работоспособность

4.4 Требования к составу и параметрам технических средств

4.4.1 Программное обеспечение должно функционировать на IBM-совместимых персональных компьютерах.

4.4.2 Минимальная конфигурация технических средств:

Процессор intel core i3, RAM 4Gb, ROM 1Tb, видеокарта nvidia geforce gt520 , монитор от 17”, материнская плата MSI, ETHERNET порт

4.5 Требования к информационной и программной совместимости

4.5.1 Программное обеспечение должно работать под управлением операционных систем Windows 7,8,10, Linux, Mac OS

4.5.2 Входные данные должны быть представлены в следующем формате:

Список, состоя.

4.5.3 Результаты должны быть представлены в следующем формате: документы в цифровом виде.

4.6 Требования к маркировке и упаковке

Требования к маркировке и упаковке не предъявляются.

4.7 Требования к транспортированию и хранению

Требования к транспортировке и хранению не предъявляются.

4.8 Специальные требования

Сгенерировать установочную версию программного обеспечение АИС, подобрать техническое обеспечение.

Оказать помощь в получении электронной подписи.

5. Требования к документации

Разрабатываемые программные модули АИС должны быть самодокументированы, т.е. тексты программ должны содержать все необходимые комментарии.

Разрабатываемая АИС должна включать справочную систему.

В состав сопровождающей документации должны входить:

* техническое задание;
* программная документация;
* техническая документация;
* программа и методики испытаний;
* руководство оператора;
* руководство администратора;
* другая эксплуатационная документация.

6. Технико-экономические показатели

Стоимость АИС – 100 000р, стоимость установки - отсутствует, стоимость обслуживания 5 000р/мес. Время установки 2 дня.

1. Стадии и этапы разработки

Разработка должна быть проведена в три стадии:

1. разработка технического задания;

2. рабочее проектирование;

3. внедрение.

# Технико-рабочий проект и результаты внедрение полученной системы

# Заключение

В заключение хотелось бы сказать, что с разнообразием информационных систем развиваются и уязвимости. Каждый год страны и компании стараются находить множество уязвимостей во всех информационных системах раньше злоумышленников для минимизации ущерба. Однако не всегда удается опережать в исследованиях злоумышленников и ущербы достигают огромных ресурсов для компаний и репутации.

Тем не менее, выполняя данный отчет, я смог познакомиться с MaxPatrol 8 и с тем, как во всем мире оценивают уязвимости, что для меня как студента направления Информационной безопасности должно быть полезно.

# Список использованных источников

<https://partners.ptsecurity.ru/>

https://www.securitylab.ru/analytics/355336.php

https://www.securitylab.ru/vulnerability/

<https://www.ptsecurity.com/ru-ru/research/threatscape/>

<https://encyclopedia.kaspersky.ru/glossary/cvss-common-vulnerability-scoring-system/>

<https://owasp.org/www-project-top-ten/>

<https://www.kb.cert.org/vuls/>