**Министерство образования и науки Российской Федерации**

федеральное государственное автономное образовательное учреждение высшего образования

**“САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ**

**УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ,**

**МЕХАНИКИ И ОПТИКИ”**

**УТВЕРЖДАЮ**

Зав. кафедрой\_\_\_\_БИТ\_\_\_\_\_\_\_\_\_\_\_

\_Закратов Игорь Алексеевич\_\_\_\_\_\_

(ФИО) (подпись)

«\_\_\_\_» «\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_» 20\_\_\_ г.

**ЗАДАНИЕ**

**НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ**

**Студент**  Олейников Иван Викторович **Группа** P3452 **Кафедра** БИТ  **Факультет** ИбиКТ  **Руководитель**\_\_\_\_Левина А.Б. , доцент, к.ф.-м.н. доцент кафедры БИТ\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(ФИО, ученое звание, степень, место работы, должность)

**1 Наименование темы:**\_\_\_\_\_Атаки по сторонним каналам\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Направление подготовки (специальность)** \_\_10.03.01 Информационная Безопасность\_\_\_\_\_

**Направленность (профиль) \_\_\_\_**Организация и технология защиты информации**\_\_\_\_\_**

**Квалификация** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_бакалавр\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(бакалавр, магистр, специалист)

**2 Срок сдачи студентом законченной работы «** 8 » «\_\_\_\_июня\_\_\_\_\_\_\_» 20\_\_17\_\_г.

**3 Техническое задание и исходные данные к работе**

а) Провести анализ различных типов атак по сторонним каналам и выбрать наиболее\_\_\_\_\_\_\_\_ перспективные с точки зрения применимости к программе верификации пароля\_\_\_\_\_\_\_\_\_\_\_\_\_

б) Раработать модель программы верификации пароля и провести эксперимент для оценки\_\_

эффективности атак по сторонним каналам\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

в) Оценить результаты эксперимента, получить выводы об эффективнсти атак по сторонним каналам\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**4 Содержание выпускной квалификационной работы (перечень подлежащих разработке вопросов)**

а) анализ различных типов атак по сторонним каналам;\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

б) выбор наиболее переспективных типов атак по сторонним каналам с точки зрения\_\_\_\_ применимости к программе валидации пароля;\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

в) разработка модели программы валидации пароля;\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

г) проведение эксперимента и оценка эффективности атак по сторонним каналам;\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**5 Перечень графического материала (с указанием обязательного материала**)

1) Слайд 1 - Титульный слайд 2) Слайд 2 - Цель работы 3) Слайд 3 - Типы атак по сторонним каналам 4) Слайд 4 - Ограничения атак по сторонним каналам 5) Слайд 5 - Атаки по времени 6) Слайд 6 - Модель атаки по времени 7) Слайд 7 - Параметры внутренней задержки 8) Слайд 8 - Параметры внутренней задержки 9) Слайд 9 - Линейная регрессия с одной независимой переменной 10) Слайд 10 - Параметры внешней задержки 11) Слайд 11 - Оценка требуемого числа измерений 12) Слайд 12 - Оценка требуемого числа измерений 13) Слайд 13 - Результат

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**6 Исходные материалы и пособия** \_\_\_\_\_не предоставлялись\_\_\_\_\_

**КАЛЕНДАРНЫЙ ПЛАН**

|  |  |  |  |
| --- | --- | --- | --- |
| №№  п/п | Наименование этапов выпускной квалификационной работы | Срок выполнения этапов работы | Отметка о выполнении, подпись руков. |
| 1 | Выбор тема ВКР | Ноябрь 2016 |  |
| 2 | Подготовка и утверждение предварительного плана работы | 15.12.16 |  |
| 3 | Изучение предметной области | 27.01.17 |  |
| 4 | Разработка и согласование с руководителем первой главы «Атаки по сторонним каналам» | 21.02.17 |  |
| 5 | Разработка и согласование с руководителем второй главы «Разработка модели» | 10.03.17 |  |
| 6 | Разработка и согласование с руководителем третьей главы «Эксперимент» | 25.04.17 |  |
| 7 | Формулировка выводов и оформление работы | 15.05.17 |  |
| 8 | Представление работы на кафедре | 23.05.17 |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**8 Дата выдачи задания «**\_6\_» «\_\_февраля\_\_» 20\_17\_г.

Руководитель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись)

Задание принял к исполнению\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ «\_6\_» «\_\_\_\_февраля\_\_\_\_\_» 20\_17\_г.

(подпись)