МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ им. В. И. ВЕРНАДСКОГО»
ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ
Кафедра компьютерной инженерии и моделирования

ОТЧЕТ ПО ПРАКТИЧЕСКОМУ ЗАДАНИЮ №1

Практическая работа
по дисциплине «Основы информационной безопасности»
студента 3 курса группы ИВТ-б-о-222(2)
Чудопалова Богдана Андреевича

09.03.01 «Информатика и вычислительная техника»

Симферополь, 2024

Рейтинг компаний в области ИБ на рынке РФ, исходя из выручки

№	Название	Выручка в 2023	Специализация
1	Лаборатория Касперского	47.7 млрд. руб.	Вендор
2	Softline	23.6 млрд. руб.	Вендор
3	Positive Technologies	22.2 млрд. руб.	Вендор
4	Солар	17.3 млрд. руб.	Вендор, интегратор
5	Код безопасность	9.2 млрд. руб.	Интегратор

Краткая характеристика каждой из компаний:

1. Компания "Лаборатория Касперского" — один из крупнейших производителей антивирусного программного обеспечения и решений в области кибербезопасности. Основана в 1997 году и имеет штаб-квартиру в Москве, Россия. Основное направление компании — защита от вирусов, вредоносного ПО, шпионских программ и других киберугроз. Включает в себя как программные решения, так и услуги по управлению безопасностью.
Основные проекты и продукты: Kaspersky Anti-Virus, Kaspersky Endpoint Security - решение для защиты корпоративных компьютеров и мобильных устройств, Kaspersky Security for Business - комплексные решения для защиты малого и среднего бизнеса, включая защиту серверов, рабочих станций и мобильных устройств. Kaspersky Cybersecurity Lab - исследовательская лаборатория, которая занимается изучением новых угроз и уязвимостей, разработкой новых технологий защиты и сотрудничеством с другими организациями в области кибербезопасности. Global Research and Analysis Team (GreAT) - команда исследователей и аналитиков, которая фокусируется на изучении и анализе киберугроз и крупных кибератак по всему миру.

2. Компания Positive Technologies — российская компания, специализирующаяся на кибербезопасности и информационных технологиях. Основное направление деятельности компании — разработка решений для защиты информационных систем и сетей от киберугроз, включая вредоносные программы, хакерские атаки и внутренние угрозы.
Основные проекты и продукты: PT Network Attack Discovery (PT NAD) - решение для обнаружения и анализа сетевых атак. PT Application Firewall (PT AFW) - система веб-защиты, которая обеспечивает защиту веб-приложений от различных типов атак. PT Industrial Security (PT IS) - решение для обеспечения безопасности промышленных систем управления (ICS/SCADA). Помогает защитить критическую инфраструктуру от киберугроз и атак на системы управления производственными процессами. PT XDR (Extended Detection and Response) - платформа для расширенного обнаружения и реагирования на угрозы, которая объединяет данные из различных источников, таких как сети, конечные устройства и облачные сервисы, для обеспечения комплексной

защиты. PT Sandbox - система для анализа подозрительных файлов и программ в изолированной среде (песочнице), что позволяет выявлять новые и неизвестные угрозы без риска для основной системы.
3. Компания Солар (Solar Security) — российская компания, специализирующаяся на решениях в области информационной безопасности и управления ИТ-инфраструктурой. Основное направление компании - предоставление решений и услуг для защиты информационных систем от различных угроз, таких как вирусы, хакерские атаки, шпионские программы и внутренние угрозы. Также компания проводит аудит и консалтинг - Солар проводит аудит информационной безопасности, оценивает уязвимости и разрабатывает рекомендации по улучшению защиты и соответствию нормативным требованиям.
Основные проекты и продукты: Solar Security - флагманский продукт компании, комплексное решение для защиты от киберугроз, включающее в себя средства для обнаружения и предотвращения атак, защиту от вредоносного ПО, системы для мониторинга и анализа безопасности. Solar Firewall - решение для защиты сети, которое включает в себя функции фильтрации трафика, управления доступом и обнаружения вторжений. Обеспечивает защиту от внешних атак и угроз.
4. Компания Код Безопасность — российская компания, специализирующаяся на решениях в области информационной безопасности и защиты данных. Основное внимание уделяется разработке программных решений, обеспечивающих безопасность корпоративных и государственных ИТ-инфраструктур. Основное направление деятельности компании включает разработку и внедрение решений для защиты от киберугроз, таких как вирусы, атаки и утечки данных. Основные проекты и продукты:
Код Секьюрити (Code Security) - комплексное решение для защиты информационных систем от угроз, включая антивирусные технологии, средства обнаружения и предотвращения атак, а также системы мониторинга и анализа угроз. Код Шифрование (Code Encryption) - решение для защиты данных через шифрование. Включает в себя как симметричное, так и асимметричное шифрование для обеспечения конфиденциальности и целостности данных.
Код SIEM (Code SIEM) - решение для управления информацией о безопасности и событиями, которое позволяет собирать и анализировать данные о событиях безопасности для своевременного реагирования на инциденты.
5. Компания Softline — это крупный российский интегратор ИТ-решений и услуг, работающий в области информационных технологий и цифровых решений, компания основана в 1993 году. Решения в области кибербезопасности от Softline:
Защита от внешних угроз - решения для защиты от атак: Softline предлагает инструменты для предотвращения внешних угроз, таких как DDoS-атаки, фишинг и вредоносные программы. Эти решения помогают защитить корпоративные сети и данные от злоумышленников.
Управление уязвимостями - Softline предоставляет решения для выявления и оценки уязвимостей в ИТ-инфраструктуре, что позволяет своевременно

принимать меры по устранению потенциальных угроз. Обнаружение и реагирование на угрозы (EDR) - системы EDR (Endpoint Detection and Response) - эти системы помогают в мониторинге, обнаружении и реагировании на инциденты безопасности на конечных устройствах, таких как рабочие станции и серверы.