|  |  |  |
| --- | --- | --- |
| Наименование | Сходства | Различия |
| SIEM | 1. Консолидация и хранение журналов событий от различных источников.  2. Предоставление инструментов для анализа событий и разбора инцидентов  3. Корреляция и обработка событий по правилам.  4. Автоматическое оповещение и инцидент-менеджмент.  5. Выявляют похожие инциденты ИБ.  6. Пользователи. | Не способны предотвращать инциденты ИБ. |
| SOC | Предотвращение инцидентов ИБ. |
| CERT | Сбор информации о событиях ИБ, классификация и нейтрализация | 1. Перед использованием необходимо получить разрешение.  2. Источники информации – только присланные клиентами данные |
| CSIRT | Существуют внутри конкретного предприятия, больше возможностей получать данные. |

|  |  |
| --- | --- |
| Наименование | Направление |
| CERT-GIB | Центр круглосуточного реагирования на инциденты информационной безопасности. Они занимаются предотвращением таких инцидентов как:  1. DoS / DDoS атаки.  2. Распространение вредоносного программного обеспечения.  3. Появление мошеннических интернет-ресурсов.  4. Несанкционированный доступ и компрометация информационных систем.  5. Инциденты, связанные с бот-сетями.  6. Фишинг и незаконное использование бренда в сети Интернет.  7. Атаки на ДБО и электронные платежные системы. |
| RU-CERT | Основная задача RU-CERT - реагирование на инциденты в области информационной безопасности.  Помимо этого в задачи RU-CERT входит: оказание содействия в анализе причин и последствий инцидентов; помощь в обращении в государственные структуры, связанные с раскрытием преступлений в области информационной безопасности; сбор статистики и генерация отчетов по инцидентам; перевод на русский язык информации о наиболее значимых уязвимостях, вирусах и т.д.; |
| GOV-CERT.RU | Осуществляет координацию действий заинтересованных организаций и ведомств в области предотвращения, выявления и ликвидации последствий компьютерных инцидентов, возникающих в ИТС органов государственной власти Российской Федерации. GOV-CERT.RU решает следующие задачи:  оказание консультативной и методической помощи при проведении мероприятий по ликвидации последствий компьютерных инцидентов в ИТС органов государственной власти РФ;  анализ причин и условий возникновения инцидентов в ИТС органов государственной власти РФ;  выработка рекомендаций по способам нейтрализации актуальных угроз безопасности информации;  взаимодействие с российскими, иностранными и международными организациями, осуществляющими реагирование на компьютерные инциденты; накопление и анализ сведений о компьютерных инцидентах.  **Создан 8-м центром ФСБ** |

|  |  |
| --- | --- |
| FinCERT | Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT) – структурное подразделение главного управления безопасности и защиты информации Банка России (ГУБиЗИ).  FinCERT осуществляет сбор информации от финансовых учреждений о кибератаках, анализирует полученные сведения и дает обратную связь кредитно-финансовым организациям о возможных угрозах информационной безопасности, разрабатывает рекомендации по отражению хакерских атак, взаимодействует с правоохранительными органами и оперативными службами ФСБ. |
| ГОССОПКА | Обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы |

**CERT-GIB**

Илья Сачков - Генеральный директор, основатель компании.

Является членом ряда международных объединений:

1. Ассоциации компьютерной криминалистики информационных систем (IISFA)
2. Ассоциации сертифицированных специалистов по борьбе с мошенничеством (ACFE)
3. Ассоциации профессионалов в области информационной безопасности RISSPA
4. Рабочей группы при ЭКС Пир-Центра по международной информационной безопасности и глобальному управлению Интернетом

**FinCERT**

Дмитрий Фролов, начальник Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России.

**RU-CERT**

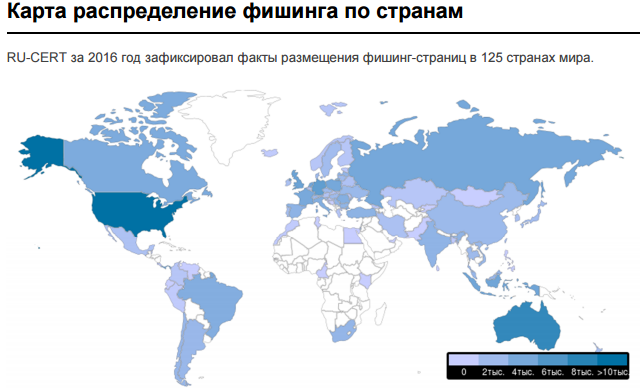
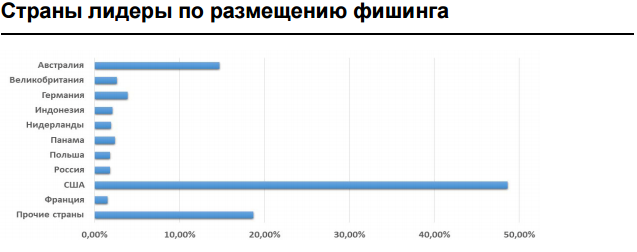


Диаграмма сервисов, подвергшихся атакам.