### **План аналитики**

### **1. Введение**

A. Определение BSS (Breach Simulation Systems)  
B. Значение BSS в контексте кибербезопасности

### **2. Состояние технологии**

A. Текущие тенденции в разработке и внедрении BSS  
B. Основные технологии и методы, используемые в BSS

### **3. Перспективы технологии**

A. Ожидаемые тренды в развитии BSS  
B. Прогнозы роста рынка BSS  
C. Возможные вызовы и ограничения в будущем

### **4. Рыночная ниша**

A. Анализ целевой аудитории и сегментации рынка  
B. Основные отрасли, использующие BSS

### **5. Производители**

A. Обзор ключевых игроков на рынке BSS  
B. Инновации и уникальные предложения от производителей

**6. Отечественное производство**

CTRLHACK

### **7. Заказчики**

A. Профили типичных заказчиков BSS  
B. Потребности и ожидания заказчиков от BSS  
C. Примеры внедрения BSS в различных организациях

### **8. Заключение**

A. Итоги анализа состояния и перспектив BSS

**1. Введение**

Breach Simulation Systems (BSS) — это специальные инструменты и платформы, предназначенные для имитации кибератак на информационные системы организаций. Основная цель BSS — выявление уязвимостей и слабых мест в системах безопасности до того, как злоумышленники смогут их использовать. Это проактивный подход к кибербезопасности, который позволяет организациям принимать меры для защиты своих данных и инфраструктуры. Можно сказать, что различные BSS составляют перечень инструментов Breach and Attack Simulation(BAS). Некоторые сведения, представленные в аналитике, будут касаться именно BAS, в связи с узконаправленностью темы BSS.

Системы симуляции нарушений в контексте кибербезопасности выполняют следующие функции:

### Оценка готовности к инцидентам

### Обучение и повышение осведомленности

### Проверка и улучшение существующих мер безопасности

### Минимизация последствий атак

### Интеграция с другими системами безопасности

### Анализ и отчетность

### Адаптация к новым угрозам

Breach Simulation Systems являются важным инструментом для повышения уровня кибербезопасности организаций, позволяя им проактивно выявлять и устранять уязвимости, обучать сотрудников и эффективно реагировать на инциденты.

**2. Состояние технологии**

Я выявил основные тенденции технологии BSS:

### Интеграция с другими решениями безопасности

### Использование искусственного интеллекта и машинного обучения

### Переход к проактивной безопасности

### Адаптация к новым типам угроз

### Упрощение и автоматизация процессов

### Фокус на отчетности и аналитике

### Соблюдение нормативных требований

Вот основные виды BSS и системы, которые в них входят:

### 1. Системы на основе сценариев

Эти BSS используют заранее определенные сценарии атак для моделирования угроз. Примеры таких систем:

* Metasploit: популярный инструмент для тестирования на проникновение, который позволяет моделировать различные атаки.
* Core Impact: платформа для тестирования на проникновение, которая поддерживает множество сценариев атак.

### 2. Системы на основе атакующих

Эти системы моделируют поведение реальных злоумышленников, используя техники и методы, которые они применяют:

* Cobalt Strike: инструмент для симуляции атак, который позволяет пользователям моделировать поведение злоумышленника.
* Red Teaming Tools: набор инструментов для проведения атакующих симуляций, включая инструменты для социальной инженерии и эксплуатации уязвимостей.

### 3. Автоматизированные системы

Эти BSS используют искусственный интеллект и машинное обучение для автоматизации процессов симуляции и анализа. Примеры:

* AttackIQ: платформа, которая позволяет проводить автоматизированные симуляции атак и оценивать готовность киберзащиты.
* Verodin: система, которая использует автоматизацию для тестирования и анализа киберзащиты.

### 4. Системы для обучения и повышения осведомленности

Эти BSS направлены на обучение сотрудников и повышение их осведомленности о киберугрозах. Примеры:

* KnowBe4: платформа для обучения сотрудников кибербезопасности, которая предлагает симуляции фишинга и тренинги.
* Cofense: система, которая помогает организациям обучать сотрудников реагированию на фишинг-атаки.

### 5. Системы для тестирования облачных и IoT-систем

С учетом роста использования облачных технологий и IoT, некоторые BSS фокусируются на моделировании угроз в этих областях. Примеры:

* CloudSploit: инструмент для оценки безопасности облачных сред, который помогает выявлять уязвимости и риски.
* IoT Security Frameworks: различные инструменты и платформы, которые помогают тестировать безопасность IoT-устройств и сетей.

### 6. Системы для анализа и отчетности

Эти BSS предоставляют расширенные возможности для анализа и отчетности, позволяя организациям оценивать результаты симуляций и делать выводы о состоянии их безопасности. Примеры:

* Splunk: платформа для анализа данных, которая может интегрироваться с BSS для анализа результатов симуляций.
* ELK Stack (Elasticsearch, Logstash, Kibana): набор инструментов для анализа и визуализации данных, который может использоваться для отчетности по результатам симуляций.

**3. Перспективы технологии**

Вот основные тенденции развития:

1. Углубленная интеграция с другими системами безопасности: Ожидается, что BSS будут все более интегрироваться с SIEM, SOAR и другими системами для создания единой экосистемы кибербезопасности.
2. Адаптация к новым технологиям: С учетом быстрого роста облачных технологий, IoT и других новых технологий, BSS будут развивать сценарии, соответствующие этим изменениям.
3. Геймификация и обучение: Внедрение игровых элементов в обучение сотрудников по кибербезопасности станет важным направлением, чтобы повысить вовлеченность и осведомленность.
4. Модели SaaS: Переход к облачным решениям и моделям подписки будет продолжаться, предлагая организациям гибкость и возможность масштабирования.
5. Регуляторные соответствия и стандарты: соответствие стандартам: Разработка BSS с учетом требований регуляторов и стандартов безопасности, таких как GDPR, HIPAA, PCI DSS и др., что поможет организациям соответствовать требованиям и избегать штрафов.
6. Облачные решения и SaaS: увеличение популярности облачных BSS, которые предлагают гибкость и масштабируемость, позволяя организациям использовать решения без необходимости значительных капитальных затрат.

Прогнозы на рост рынка Breach Simulation Systems (BSS) в ближайшие годы выглядят весьма оптимистично, и несколько факторов способствуют этому:

1. Увеличение киберугроз: С ростом числа кибератак и утечек данных организации осознают необходимость в проактивных мерах защиты. Это ведет к увеличению спроса на решения, которые помогают моделировать и тестировать киберугрозы.
2. Развитие технологий: Внедрение искусственного интеллекта и машинного обучения в BSS позволяет создавать более эффективные и адаптивные системы. Это способствует росту интереса со стороны компаний, стремящихся улучшить свои стратегии киберзащиты.
3. Регуляторные требования: Ужесточение норм и стандартов в области кибербезопасности, таких как GDPR, HIPAA и других, побуждает организации инвестировать в BSS для соответствия требованиям и минимизации рисков.
4. Увеличение бюджета на кибербезопасность: Многие компании увеличивают свои бюджеты на кибербезопасность, что позволяет им вкладываться в новые технологии и решения, включая BSS.
5. Рост удаленной работы: Пандемия COVID-19 привела к увеличению удаленной работы, что создало новые уязвимости. Компании ищут способы защитить свои сети и данные, что также способствует росту рынка BSS.

Приблизительные прогнозы:

Согласно исследованию «Automated Breach and Attack Simulation (BAS) Market Size And Forecast» рынок BAS оценивался в 130,82 млн долларов США в 2019 году и, по прогнозам, достигнет 1572,59 млн долларов США к 2027 году, увеличиваясь в среднем на 36,47 % с 2020 по 2027 год. По данным [прогноза развития рынка кибербезопасности в РФ на 2023-2027 годы](https://www.csr.ru/upload/iblock/0da/cl25xkzy12if5l4xs425yi25ezp1a11z.pdf) от ЦСР, рост объема рынка кибербезопасности за период 2022–2027 года ожидается в районе 24 % CAGR. При этом на основе данных о продажах дистрибьютора «Тайгер Оптикс» можно предполагать, что объём рынка BAS в России составляет порядка 2–2,5 млн долларов США в годовом выражении.

Источник: <https://www.anti-malware.ru/analytics/Market_Analysis/Breach-and-Attack-Simulation-Market-Overview#part4>

**4. Рыночная ниша**

* Целевой рынок: Основные целевые клиенты BSS включают крупные корпорации, финансовые учреждения, государственные организации, а также малый и средний бизнес, которые нуждаются в повышении уровня кибербезопасности.
* Отрасли: BSS востребованы в различных отраслях, включая финансы, здравоохранение, технологии, энергетику и государственные учреждения.

**5. Производители**

Некоторые из ведущих производителей технологий симуляции атак включают:

1. Cymulate: Платформа, предлагающая симуляции атак и оценку уязвимостей.
2. SafeBreach: Предоставляет решения для симуляции кибератак и анализа уязвимостей.
3. AttackIQ: Платформа для тестирования безопасности и симуляции атак, ориентированная на улучшение защиты.
4. Verodin: Инструменты для симуляции атак и анализа инцидентов в реальном времени.
5. Red Canary: Специализируется на обнаружении и реагировании на угрозы, включая симуляцию атак.

**6. Отечественное производство**

В России сегмент рынка продуктов Breach and Attack Simulation находится на ранней стадии развития. Продукты только появляются на рынке, многие компании только проводят пилотные тесты, однако интерес со стороны заказчиков увеличивается. При этом на российском рынке присутствуют как отечественные вендоры (ООО «Контролхак»), так и зарубежные (Cronus Cyber Technologies, Cymulate, Pcysys, Picus Security). По мнению Романа Богомолова, в России не более 10 заказчиков используют подобные системы на текущий момент.

Источник: <https://www.anti-malware.ru/analytics/Market_Analysis/Breach-and-Attack-Simulation-Market-Overview#part4>

<https://www.anti-malware.ru/analytics/Technology_Analysis/Breach-and-Attack-Simulation>

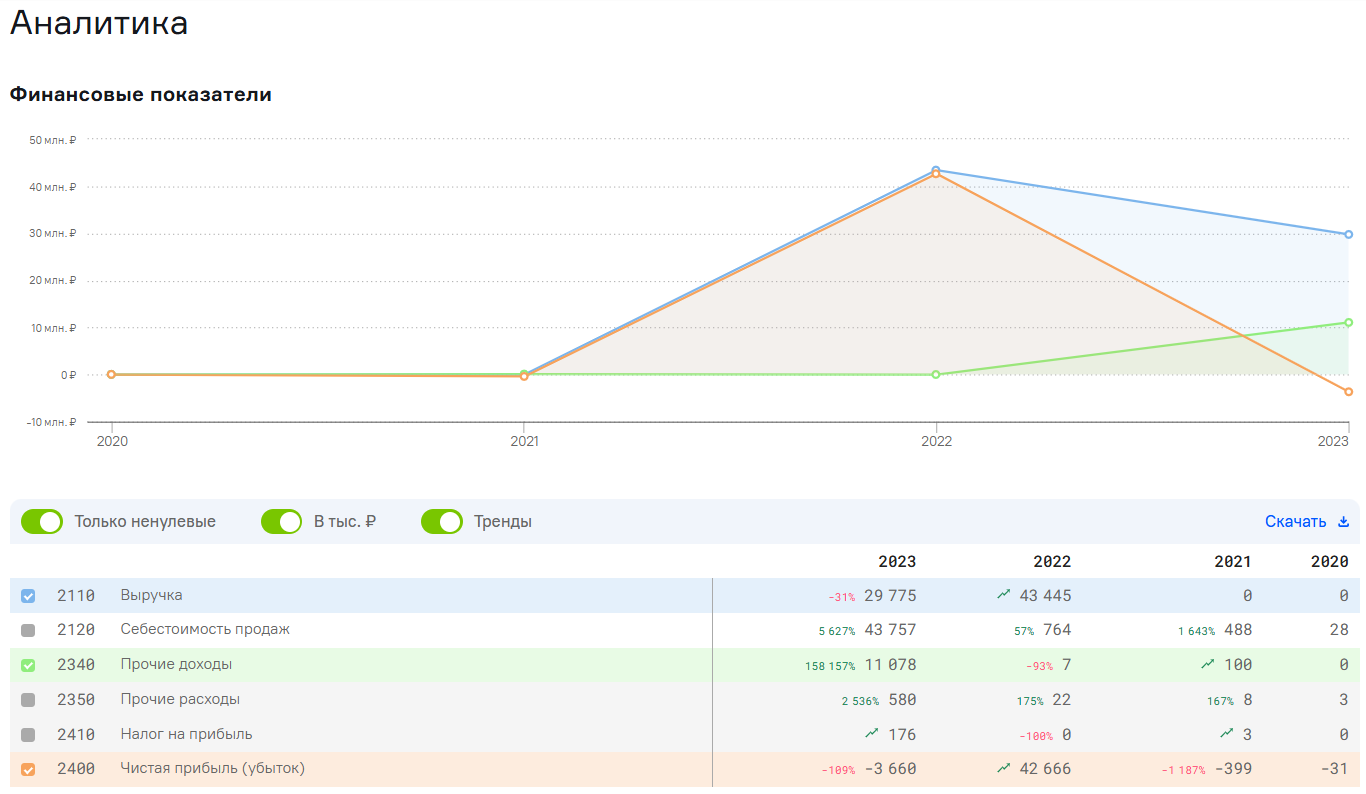
CTRLHACK – платформа автоматической симуляции атакующих хакерских техник, являющаяся российской разработкой. Она поддерживает как B2B, так и B2G модели, а также входит в Единый государственный реестр отечественного ПО. К примеру, CTRLHACK поддерживает такую BSS как Red Team.

Сайт компании: <https://ctrlhack.ru/>

Продуктом данной компании является программное обеспечение CtrlHack Base Platform - платформа симуляции кибератакующих техник непосредственно в инфраструктуре организации. Платформа позволяет проводить симуляции различных действий, имитирующих действия хакеров, для всех стадий выполнения кибератак. Симуляции выполняются в автоматическом режиме. Результаты выполнения симуляций позволяют оценить работу средств защиты информации и повысить эффективность детектирования кибератакующих техник на уровне правил детектирования в системах класса SIEM.

Источник: <https://navigator.sk.ru/orn/1123572>

ГОСУДАРСТВЕННАЯ РЕГИСТРАЦИЯ ПРОГРАММЫ ДЛЯ ЭВМ: <https://www1.fips.ru/fips_servl/fips_servlet?DB=EVM&DocNumber=2023665564&TypeFile=html>

Это данные, предоставленные SK Сколково касательно финансового положения CTRLHACK.

Источник: <https://navigator.sk.ru/orn/1123572>

**7. Заказчики**

* Корпорации
* Государственные учреждения
* Малый и средний бизнес

Вот некоторые конкретные примеры:

1. Финансовые учреждения:

* Goldman Sachs: Инвестиционный банк, который внедряет передовые технологии для защиты своих систем от киберугроз.
* JPMorgan Chase: Один из крупнейших банков в мире, который использует технологии симуляции атак для повышения уровня киберзащиты.

1. Государственные организации:

* Министерство обороны США: Использует симуляцию атак для тестирования систем безопасности и защиты национальной инфраструктуры.
* Федеральное бюро расследований (ФБР): Активно применяет симуляцию атак для оценки уязвимостей в своих системах.

1. Здравоохранение:

* Kaiser Permanente: Одна из крупнейших медицинских организаций в США, использующая технологии для защиты данных пациентов.
* Mayo Clinic: Здравоохранительное учреждение, которое также активно работает над повышением уровня кибербезопасности.

1. Технологические компании:

* Google: Использует симуляцию атак для защиты своих облачных сервисов и пользовательских данных.
* Apple: Применяет технологии симуляции атак для тестирования безопасности своих устройств и сервисов.

### 

### **8. Заключение**

Рынок BSS находится в состоянии динамичного роста и трансформации, предлагая множество возможностей для компаний, которые готовы адаптироваться к изменениям и внедрять инновационные технологии. Успех в этом сегменте будет зависеть от способности компаний предлагать гибкие, безопасные и ориентированные на клиента решения.