Тренды в сфере информационной безопасности: Опыт Фонда Сколково

Михаил Стюгин

Руководитель направления «Информационная безопасность»

Фонд «Сколково»

Рыночные тренды 2018-2019

Российский рынок информационной безопасности 82 млрд. руб.

Мировой рынок $114,2 млрд.

Market Segment	2018	2019
Application Security	2,7	3
Cloud Security	0,3	0,5
Data Security	3,1	3,5
Identity Access Management	9,8	10,6
Infrastructure Protection	14,1	15,3
Integrated Risk Management	4,3	4,7
Network Security Equipment	12,4	13,3
Other Information Security Software	2	2,3
Security Services	58,9	64,2
Consumer Security Software	6,4	6,7
Total	114,2	124,1

Тренды в области ИБ (угрозы)

Мировая экспертиза

1. IoT devices (IoT botnets)

Наиболее быстроразвивающийся сегмент. Прогнозируется рост рынка IoT к 2024 году до $6,5 трлн.

2. Attacks on critical national infrastructure

Индустриальный интернет вещей, энергосети, приборы контроля и учета и пр.

3. Crypto-jacking

Использование ресурсов для майнинга. По данным отчета Webroot с ним связано 35% всех угроз ИБ.

4. Ransomware

Программы-вымогатели, шифровальщики
Развитие услуг malware-as-a-service

5. Blackmail

Использование персональной информации из соц. сетей и корпоративных источников с целью шантажа

6. APT groups, state-sponsored attacks

Группы злоумышленников, имеющие крупных инвесторов и прорабатывающие целевые атаки в течении месяцев или лет

7. Encrypted traffic malware

Передача зловредов внутри зашифрованного трафика

8. AI-assisted imposters

Использование искусственного интеллекта для генерации поддельных фото, документов, текстов и пр.

Тренды в области ИБ (решения)

Мировая экспертиза

1. Compliance

Увеличение доли процессов ИБ, регулируемых нормативными и законодательными документами

2. Data-centric security

Развитие подхода DCSM (Data Centric Security Model), устанавливающего фокус на присвоении данным определенного уровня безопасности.

3. Cloud-based security platforms

Увеличение доли облачных сервисов как инструмента в области кибербезопасности

4. Blockchain for IT security

Использование блокчейна для построение инструментов CISO, единых баз уязвимостей и контроля целостности

5. AI and advanced analytics

Увеличение доли автоматизации процессов в обеспечении процессов ИБ, обработки инцидентов.

6. Zero trust is maturing into digital trust

Трансформация сложной в реализации концепции нулевого доверия к цифровому доверию, путем использование «цифровых отпечатков» пользователей

Стартапы ИБ и венчурные инвестиции

Мировой рынок

Обзор 150 наиболее быстрорастущих стартапов в области ИБ

Ключевые темы роста 2018 года

Искусственные иммунные системы – технологии позволяющие определять «типичное» поведение устройств, приложений и процессов, выявляя аномалии и предотвращая их.

DarkTrace - От $30 млн. инвестиций до оценки в $1,25 млрд.

Антифишинг и борьба с мошенническими рассылками по email.

Повышение защищенности информационных систем путем защиты их от исследования – инструменты Deception и Moving Target Defense

---

Threat Intelligence – анализ уязвимостей и мониторинг процессов в информационных системах с использованием AI и ML

Географическое распределение:
United States – 88%, из них из Калифорнии – 83%
Israel – 5%
Другие страны – 7%

Технологическое распределение:
67% стартапов используют технологии Machine learning и Artificial Intelligence
24% стартапов ориентированы на модель data-centric security

Стартапы ИБ и венчурные инвестиции

Мировой рынок

Наиболее яркие кейсы ИБ в 2018

AGARI

Один из мировых лидеров борьбы с фишинговыми рассылками, позволяющий «понимать» реального отправителя писем путем применения запатентованных алгоритмов идентификации писем и использования сети глобальной телеметрии email-писем.

Bromium

Защита конечных устройств в противоположность традиционной концепции detect-to-protect. Когда каждая из уязвимостей располагается в собственном контейнере виртуальной машины, пользователь может без опасений открывать ссылки в интернете, запускать приложения или документы из открытых источников.

illusive
Advanced attacker deception

Создание альтернативной реальности на уровне сетевых протоколов и интерфейсов, распределенных в реальной сети предприятия. Атакующий попадает в «альтернативную» сеть в результате исследования сети, где система исследует уже его самого.

DARKTRACE

Определение процесса нормального функционирования устройств и пользователей в системе с целью определения «паттернов жизни» и отклонения от них (искусственные иммунные системы)

По указанным кейсам на сегодняшний день в России не представлено каких-либо решений , позволяющих закрыть обозначенные проблемы заказчика.

Развитие направления кибербезопасности в Сколково

Участниками Сколково являются более 70 компаний с решениями в области кибербезопасности, представляющие продукты по большинству ключевых направлений и трендов развития отрасли ИБ.

Network Security (IDS/IPS, NGFW, APT)

SIEM, ML/AI-аналитика

Защита КИИ, 187-ФЗ

AntiFraude, AntiPiracy

Шифрование, ЭЦП

Фильтрация трафика и AntiDDoS

Web Security

IDM, PIM, 2FA

DLP, DRM

Развитие направления кибербезопасности в Сколково

Показатели развития направления ИБ в 2017 году:

Выручка полученная стартапами
более 2,5 млрд.руб.
(рост в сравнении с 2016 – 73%)

Количество созданных рабочих мест
более 800
(рост в сравнении с 2016 – 35%)

Подано 45 международных заявок на патентование
(рост в сравнении с 2016 годом – 17%)

Ожидаемый рост по выручке в 2018 году – 30%

Всего за последние 3 года

Было привлечено более
0,5 млрд. рублей частных инвестиций

Выдано 11 грантов на сумму
224 млн.рублей
(InfoWatch, GroupIB, GroupIB TDS, Remparo, Wallarm, WorksPad, Крибрум, SafeTech, OzForensics, SolidWall)

Выдано 53 микрогранта
на сумму
17,5 млн.рублей.

Успехи резидентов Сколково

Победы в конкурсах и прохождение отбора в престижные акселераторы

АСП Лабс - Программный комплекс «АРКАН». Первое решение по межсетевому экранированию, получившее сертификат ФСТЭК России на соответствие документу «Профиль защиты межсетевых экранов типа Д четвертого класса защиты. ИТ.МЭ.Д4.ПЗ» и является первым МЭ типа Д для реализации требований ФЗ-187.

Wallarm - Компания открыла офис в Силиконовой долине и в 2018 году привлекла 8 млн. долл. от инвестиционного фонда Toba Capital. По итогам 2017 года компания вошла в список пяти тысяч самых быстро растущих компаний в Северной Америке Inc. 5000 под номером 805.

Прософт-Биометрикс - Компания BioSmart s.r.o, европейское представительство сколковского участника «Прософт-Биометрикс», объявила о завершении крупного проекта по внедрению технологий биометрической идентификации в чешские дата-центры для создания безопасного контрольно-пропускного режима.

SafeTech - Программно-аппаратный комплекс «КриптоПро DSS» с модулем аутентификации myDSS недавно был сертифицирован ФСБ. В результате долгожданного прорыва в России впервые появилась легальная технология электронного документооборота с помощью мобильного приложения на смартфоне.

VisionLabs - Стала одним из мировых лидеров в области создания систем компьютерного зрения и машинного обучения. Флагманским продуктом компании является платформа распознавания лиц LUNA, которую уже сегодня используют более 40 банков и национальных кредитных бюро в России и странах СНГ. В 2018 году запустила систему распознавания лиц в одной из московских школ.

Успехи резидентов в 2018 году

Анализ тенденций в области инноваций ИБ

Ключевые точки роста (мировой рынок)	Сопоставление (отечественный рынок)
Искусственные иммунные системы	Нет решений
Инструменты Deception и MTD	Нет решений
Антифишинг и борьба с мошенническими рассылками	Нет тенденции
Threat Intelligence	Точка роста
Защита endpoint через виртуализацию	Нет решений
Криптокошельки + блокчейн в ИБ	Нет решений
Автоматизация аудита и конфигурации под требования регуляторов	Точка роста
Data-centric security approach	Нет тенденции
Cloud-based security	Нет тенденции
SOC as a Service	Точка роста
UEBA	Нет решений
Безопасность IoT	Нет решений

Рост, который можно видеть на уровне проектов ранних стадий (конкурсы идей, технологий, заявки на статус участника и пр.)

- Безопасность IoT
- Forensics, проверка контрагентов (BigData – аналитика, KYC)
- Решение на основе блокчейна
- Защита через виртуализацию
- AI в области анализа неизвестного
- UEBA

Особенности развития стартапов в России

- Сложность геополитической ситуации. Регистрация зарубежных юр.лиц с максимальным дистанцированием от отечественных
- Большинство венчурных инвестиций на российском рынке ИБ с госучастием
- Закрытость зарубежного венчурного рынка для отечественных решений ИБ
- Практически полное отсутствие фундаментальных ИБ-разработок без присутствия конечного заказчика
- Отсутствие внутренней конкуренции по сегментам рынка ИБ
- Импортозамещение и реестр отечественного ПО

Поиск высокотехнологичных решений ИБ – конкурс Skolkovo Cybersecurity Challenge, реестр инженерно-технических задач

Реализация механизмов продуктивной конкуренции – максимально быстрый выход на зарубежные рынки, включая организацию бизнес-миссий и помощь в участии в зарубежных мероприятиях

Формирование спроса на инновации в среде крупных промышленных и государственных предприятий – запуск совместных акселераторов пилотирование и внедрение решений в реальной инфраструктуре

Михаил Стюгин

Руководитель направления «Информационная безопасность»
Фонда «Сколково»

г. Москва, ул. Большой бульвар 42, стр.1

MStyugin@sk.ru

+7 977 977 1519
+7 495 956 0033 (3587)