Современные тенденции защиты информации и актуальные уязвимости в распределенных информационно-телекоммуникационных системах Российской Федерации

Остапенко Григорий Александрович
первый заместитель руководителя департамента связи и массовых коммуникаций Воронежской области

Президент определил 5 направлений кибербезопасности

Совершенствование государственной системы **обнаружения, предупреждения** и ликвидации последствий кибератак на российские сети

Развитие ГОССОПКА

Объективное использование иностранных ПАК

Максимальное снижение рисков, которые возникают в связи с «объективной необходимостью использовать **иностранные программы** и телекоммуникационное оборудование»

Международное сотрудничество

ООН, БРИКС, АТЭС, ОДКБ, СНГ

Киберзащита органов власти

Повышение защищенности информационных систем и сетей связи госорганов

Безопасный интернет

Повышении **безопасности** и надежности работы российского интернета

«Анализ развития ситуации в информационном пространстве свидетельствует о резком обострении противоборства в данной сфере, которое из разряда демонстрации технологического превосходства переходит в системное массированное информационное воздействие с заведомо деструктивными целями», - подчеркнул секретарь Совбеза.

Проект финансирования направления кибербезопасности

	Всего, руб.	2018 г.	2019 г.	2020 г.
Планируемый результат/сумма затрат, млн руб	116 846,9	39 461,9	55 153	22 232
Обеспечить устойчивость и безопасность функционирования информационных систем и технологий	34 333	7 085	12 529	14 719
Информационная система обеспечения целостности, устойчивости и безопасности функционирования российского сегмента сети интернет (**ГИС "Интернет"**)	21 460	6 760	14 700	0
Обеспечение **технического контроля** законности обработки данных в сетях связи, ЦОД и информационных системах	20 000	10 000	10 000	0
Элементы инфраструктуры **единого пространства доверия** электронной подписи	8 659	1 839	2 815	4 005
Стандарты безопасной разработки приложений	6 015	3 005	3 010	0
Система получения знаний в области ИБ на основе национальной электронной библиотеки	2 410	310	2 100	0
Законодательные требования к программно-техническим средствам защиты от компьютерных атак, включая **ddos-атаки**, противоправного конттента, **средствам анализа** и **фильтрации трафика** на сетях связи	2 370	870	1 500	0
Маршрутизация российского интернет-трафика преимущественно по территории РФ	2 350	1 200	1 150	0
Стимулирование разработки отечественных комплексов обеспечения безопасности для оборудования IoT	2 034	13	1 011	1 010
Реализована система управления рисками информационной безопасности при интеграции в международную цифровую экономику	1 650	550	550	550
Использование отечественных операционных систем	768	236	236	296
Создание средств информационной безопасности для целей цифровой экономики	600	500	100	0
Создание системы **добровольного декларирования** уровня безопасности продуктов и услуг ИКТ (Декларирование информационной безопасности)	520	120	200	200
Создание информационного ресурса, обспечивающего гражданам РФ доступ к информации о случаях использования их персональных данных, а также возможность отказа от такого использования	440	0	440	0
Создание системы **экспертных организаций** в области компьютерной криминалистики	400	300	50	50
Принятие национальных стандартов обработки **больших данных**. Система добровольной сертификации на соответствие этим стандартам.	400	0	400	0
Анализ существующей системы **подготовки** квалифицированных **специалистов** в области информационной безопасности	360	240	70	50
Разработка механизмов инструментального контроля использования **больших данных**	350	0	150	200

2018

Накоплена база знаний по актуальным угрозам и уязвимостям различных уровней

4 ДЕПАРТАМЕНТ СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ

РОСТ УЯЗВИМОСТЕЙ

ФСТЭК России: угрозы и уязвимости

Уязвимости системного программного обеспечения

Уязвимости прикладного программного обеспечения

Уязвимости используемых телекоммуникационных протоколов

Стационарные аппаратно-программные комплексы

Мобильные платформы

https://bdu.fstec.ru/threat

Информационная деятельность ФСТЭК России

25 февраля 2018	Об уязвимостях центральных процессоров производства **Intel, AMD и ARM**
25 октября 2017	Об уязвимости микропрограммного обеспечения **Intel Management Engine**
2 июля 2017	О мерах по защите информации, направленных на нейтрализацию угроз безопасности информации, связанных с проникновением и распространением вредоносного программного обеспечения **WannaCry, Petya, Misha** и их модификаций
20 июля 2016	О применении сертифицированных по требованиям безопасности информации средств антивирусной защиты «Антивирус Касперского 6.0 для WindowsServers» и «Антивирус Касперского 6.0 для WindowsWorkstation» в условиях прекращения их поддержки разработчиком
19 июля 2016	Об уязвимостях в сертифицированных средствах защиты информации **Dallas Lock 8.0**
12 апреля 2016	Об уязвимостях в сертифицированных средствах защиты информации **Secret Net** и мерах по их нейтрализации

Информационные сообщения Cisco

Critical Vulnerabilities

Oracle CPU, OIT Vulnerabilities Multiple CVEs Jan 18th	OpenSSL Vulnerabilities Multiple CVEs Jan 26th	OpenSSL Vulnerabilities CVE-2017-3733 Feb 6th	Apache Struts 2 Remote Code Execution Vulnerabilities CVE-2017-5638 Mar 6th
Microsoft Windows Graphics CVE-2017-0108 Mar 14th	Microsoft Windows Server Message Block Service Arbitrary Code Execution Vulnerabilities CVE-2017-0145 Mar 14th	Network Time Protocol Vulnerabilities Multiple CVEs Mar 21st	Microsoft Internet Information Services (IIS) WebDAV CVE-2017-7269 Mar 29th
Microsoft Office (Dridex Exploiting) CVE-2017-0199 Apr 11th			

Attack Activities

WikiLeaks Vault 7 Release Multiple CVEs Mar 7th	WannaCry Activity MS17-010 Multiple CVEs May 17st
Operation Cloud Hopper Sustained Global Campaigns Apr 6th	Shadow Brokers Group Disclosure of Equation Exploits Apr 8th
Apache Struts REST Plug-in XML Processing Arbitrary Code Execution Vulnerability CVE-2017-9805 Sep 6th	Microsoft .NET Framework Arbitrary Code Execution Vulnerability CVE-2017-8759 Sep 12th

Анализ уязвимостей ФСБ России по ИТКС

Повышение привилегий

Устаревшее ПО

VPN

Поиск уязвимостей в ИТКС и ИС

- Отказы в обслуживании (DNS, DTLS для OpenSSL…)
- Обход ограничений доступа
- Уязвимости в коде (PHP, MySQL…)
- Межсайтовое выполнение сценариев

Обход ограничений безопасности

Ненадежная криптография

- Несанкционированные HTTP-запросы
- Удаленное выполнение кода (связанное с SQL Server…)
- Уязвимости в Apache HTTP Server

Выработка рекомендаций

- Замена SSL-сертификата сервера на новый, использующий алгоритм SHA-256
- Использование защищенного протокола HTTPS
- Доработка исходных кодов приложения с целью обеспечения фильтрации данных поступающих от пользователей
- Обновление программного обеспечения на актуальную версию
- …

Развитие целевых компьютерных атак

Advanced persistent threats (APT-атаки)

2016-2017 годы – годы вредоносных программ-вымогателей

Финансовые потери от сетевого мошенничества с использованием корпоративной электронной почты в 2016 году составили 3 млрд долларов США, при том число уязвимостей в различном ПО составило порядка 500

По данным **TrendMicro**:
с первого полугодия 2016 года **количество программ-вымогателей выросло на 172%.**
По данным **Symantec** в 2017 году рост числа вымогателей продолжился (29 новых групп)

Выросло количество уязвимостей, обнаруженных в Adobe FlashPlayer и платформах для Интернета вещей

Современные наборы эксплойтов используют старые уязвимости

Обновление вредоносных программ для PoS-терминалов привело к росту сетевых атак. Появилась вредоносная программа FighterPoS: функционирует как червь, распространяясь через сеть PoS-терминалов.

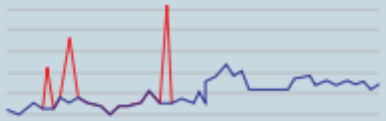
Применение машинного обучения при поиске угроз

Known-Known
Detect the exactly known infection, as seen before

Known-Unknown
Detect previously unseen variations of known threats, subfamilies or related new threats

Unknown-Unknown
Detect zero-days, unrelated to any known malware

Threat Type vs. Suitable Detection Technique

	Static Signatures	Dynamic Signatures	Behavioral Signatures	High-Level Patterns	Unsupervised Anomalies
Examples	Concrete malicious domain name associated to trojan **server1.39sIxu3bw.ru**	Houdini RAT telemetry pattern **regex: .*/i[a-z]-(ready|ri-noy|gnfoh)**	Two illustrative found instances **hxxp://crazyerror.su/b/opt/8681BAE3DB3A2F9D446CD5E3** **hxxp://50.63.147.69:8080/b/req/3D111E6B21F373015C646CA4**	Generic characteristics of suspicious traffic 	Expected vs. unexplained and unexpected 
	Ручное определение. Инструментальная поддержка. Точное совпадение предопределенных символов или их числовой последовательности. Описания доступные для оператора.	**Ручное определение. Инструментальная поддержка.** Соответствие предопределенных правил (регулярных выражений). Описания доступные для оператора.	**Машинное обучение. Согласование машинного обучения по правилам.** Приведение поведенческих моделей в преобразованное пространство объектов.	**Самостоятельное машинное обучение. Высокоуровневые шаблоны.** Обучение отличиям от общего поведения.	**Самостоятельное машинное обучение. Обучение моделям неизвестного поведения.** Отличия могут быть существенными.

* Cisco 2018 Annual Cybersecurity report

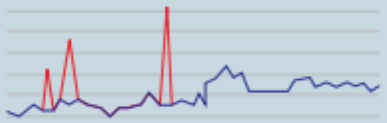
Современные Кибератаки

Better Precision and Explainability, Simplicity of Proof ← Technique Trade-Off

Better Recall, Scalability, Applicability to Encrypted Data, Ability to Detect Zero-Days →

Please note: scaling statements refer to human time required to maintain detection system

Please note: this diagram represents a simplified illustration of machine learning capabilities in security

	Static Signatures	Dynamic Signatures	Behavioral Signatures	High-Level Patterns	Unsupervised Anomalies
Examples	Concrete malicious domain name associated to trojan **server1.39slxu3bw.ru**	Houdini RAT telemetry pattern **regex: .*/i[a-z]-(ready|ri-noy|gnfoh)**	Two illustrative found instances **hxxp://crazyerror.su/b/opt/8681BAE3DB3A2F9D446CD5E3** **hxxp://50.63.147.69:8080/b/req/3D111E6B21F373015C646CA4**	Generic characteristics of suspicious traffic 	Expected vs. unexplained and unexpected 
	Очень высокая точность	**Очень высокая точность**	**Высокая точность**	**Приемлемая точность**	**Низкая точность**
	1. В одинаковых случаях работает одинаково. 2. Легкое обучение. 3. Не масштабируется. 4. Необходима «ручное» определение (реагирование) 5. Не работает с шифрованными данными - MiTM	1. Подстраивается под шаблон (ограничение по настройке). 2. Легкое обучение. 3. Масштабируется плохо. 4. Необходима «ручное» определение (реагирование) 5. Не работает с шифрованными данными - MiTM	1. Работа по поведенческим сигнатурам. Удобно для поиска неизвестных вредоносов. 2. Доступное обучение. 3. Масштабируется неплохо. 4. Обучаемы для реагироваия. 5. Работает с шифрованными данными без расшифровки.	1. Возможность поиска уязвимостей нулевого дня и целевых атак. 2. Ограниченное обучение. 3. Масштабируется хорошо. 4. Обучаемы для реагирования. 5. Работает с шифрованными данными без расшифровки.	1. Реагирование на нестандартное поведение. Высокий риск ложного срабатывания. 2. Сложное обучение. 3. Масштабируется хорошо. 4. Автоматическое обучение по данным (статистика). 5. Работает с шифрованными данными без расшифровки.

* Cisco 2018 Annual Cybersecurity report

Опасности реализации DDOS от IOT-устройств

В 2012 году произведено 9 млрд IoT устройств и ожидается, что в 2020 году их будет не менее 24 млрд

70%

Согласно оценкам Cisco, процент интернет-трафика, генерируемого устройствами, не являющимися персональными компьютерами, увеличится почти до 70% к 2019 г.

Вычислительные мощности домашних роутеров превышают профильные требования к данным устройствам

IoT-устройства, скомпрометированные вредоносными программами, могут стать платформой для нежелательного трафика

Университет Твенте, Нидерланды:

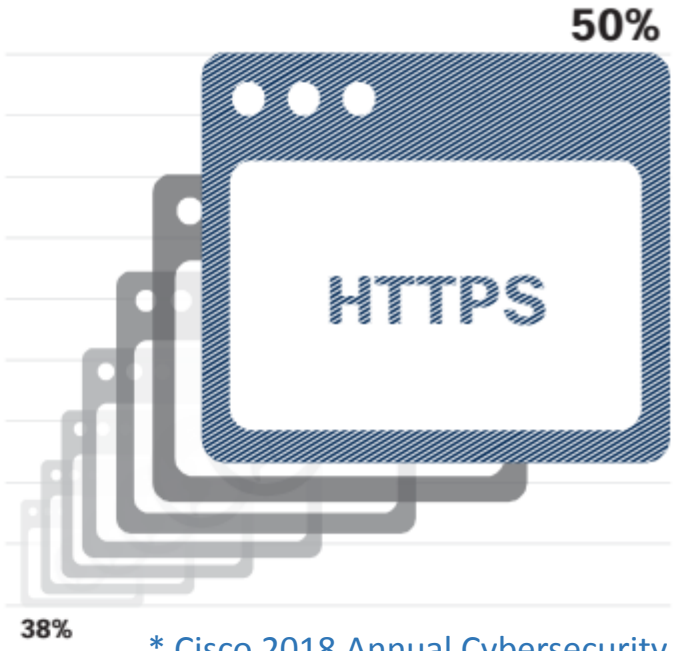
Используя среднюю скорость соединения 15,85 Мбит/с (данные операторов связи), для генерирования DDOS-атаки шириной 586 Гб/с требуется приблизительно 37 890 устройств

Ширина DDoS-атаки при учете сетевой активности 24 млрд IoT-устройств (Тб/с)

		Devices accessible					
		1%	10%	25%	50%	75%	100%
Devices usable	1%	36.28	362.78	906.94	1,813.89	2,720.83	3,627.78
	10%	362.78	3,627.78	9,069.44	18,138.89	27,208.33	36,277.77
	25%	906.94	9,069.44	22,673.61	45,347.21	68,020.82	90,694.43
	50%	1,813.89	18,138.89	45,347.21	90,694.43	136,041.64	181,388.85
	75%	2,720.83	27,208.33	68,020.82	136,041.64	204,062.46	272,083.28
	100%	3,627.78	36,277.77	90,694.43	181,388.85	272,083.28	362,777.71

Рост HTTPS-трафика в 2017 году

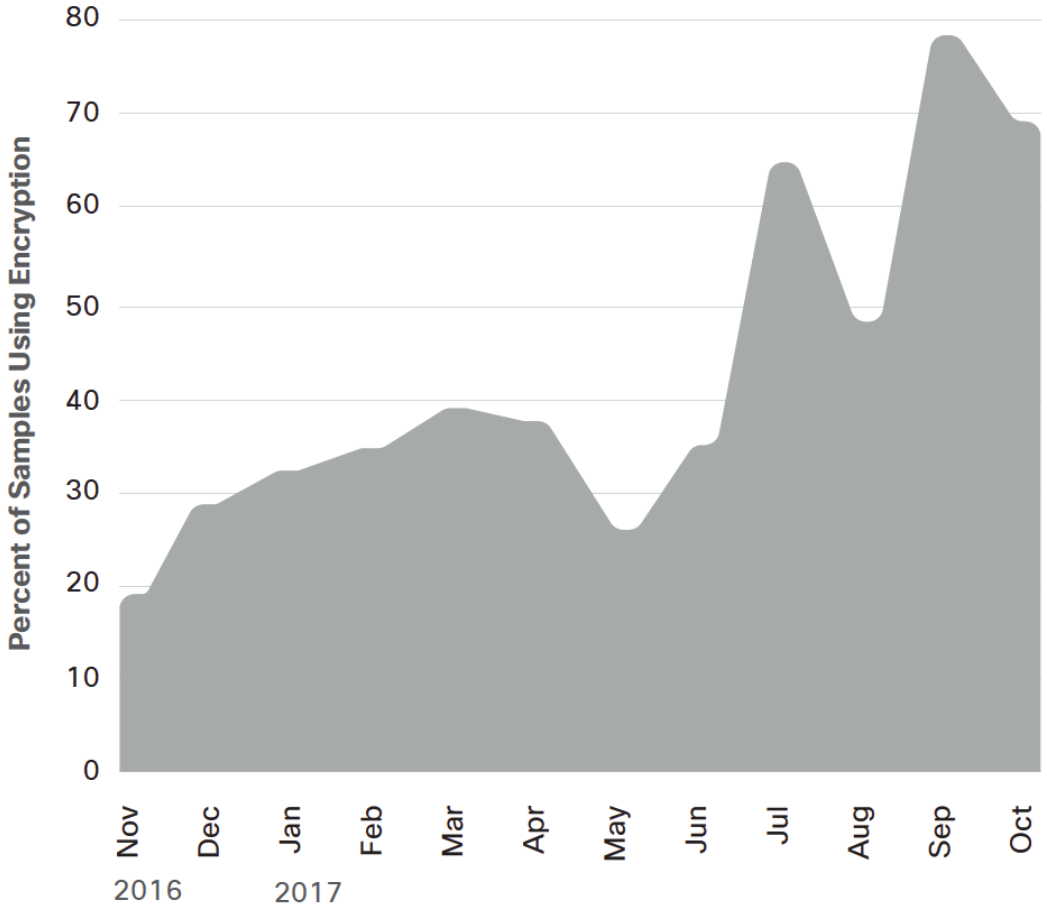
По данным Cisco 50% глобального веб-трафика было зашифровано по состоянию на октябрь 2017 года



* Cisco 2018 Annual Cybersecurity report

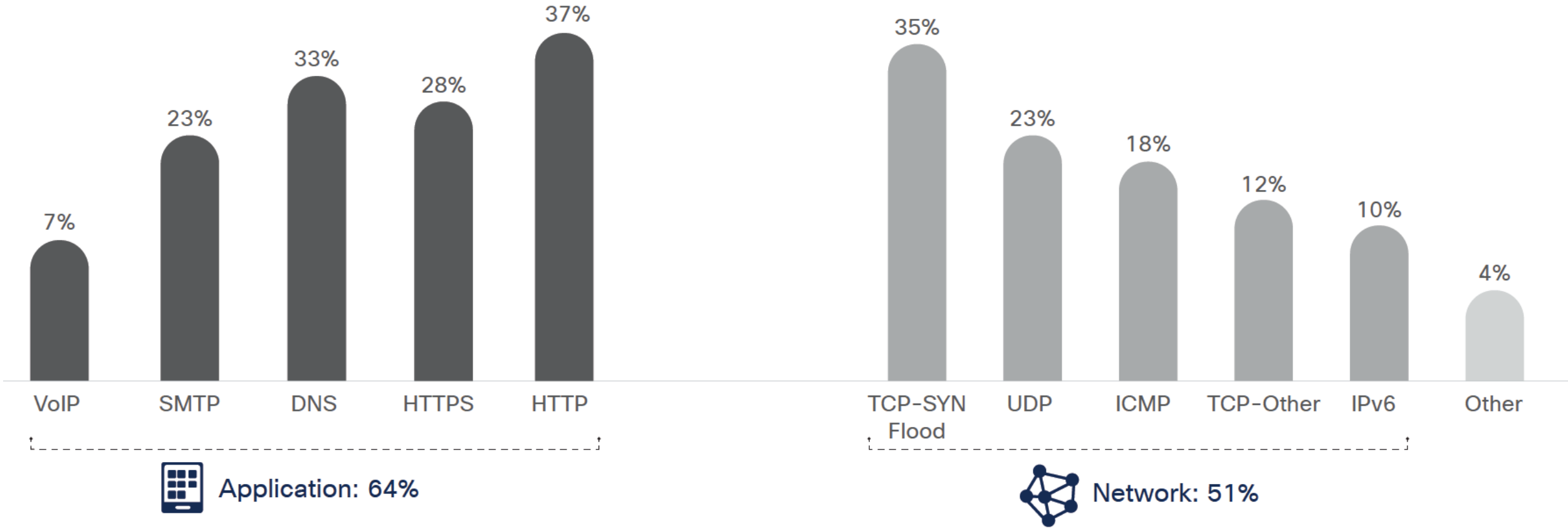
К октябрю 2017 года в 12 раз выросло количество HTTPS трафика по сравнению с ноябрем 2016 года

Увеличилось число вредоносных воздействий в зашифрованных сетях



Рост DDOS-атак на уровне приложений

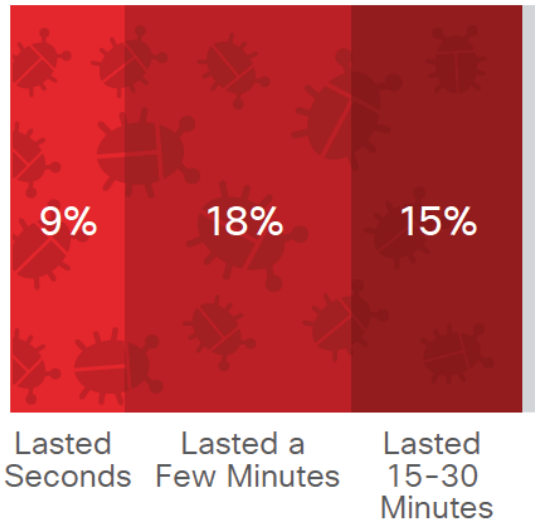
По данным Cisco происходит рост количества атак, направленных в сторону использования уязвимостей прикладного программного обеспечения



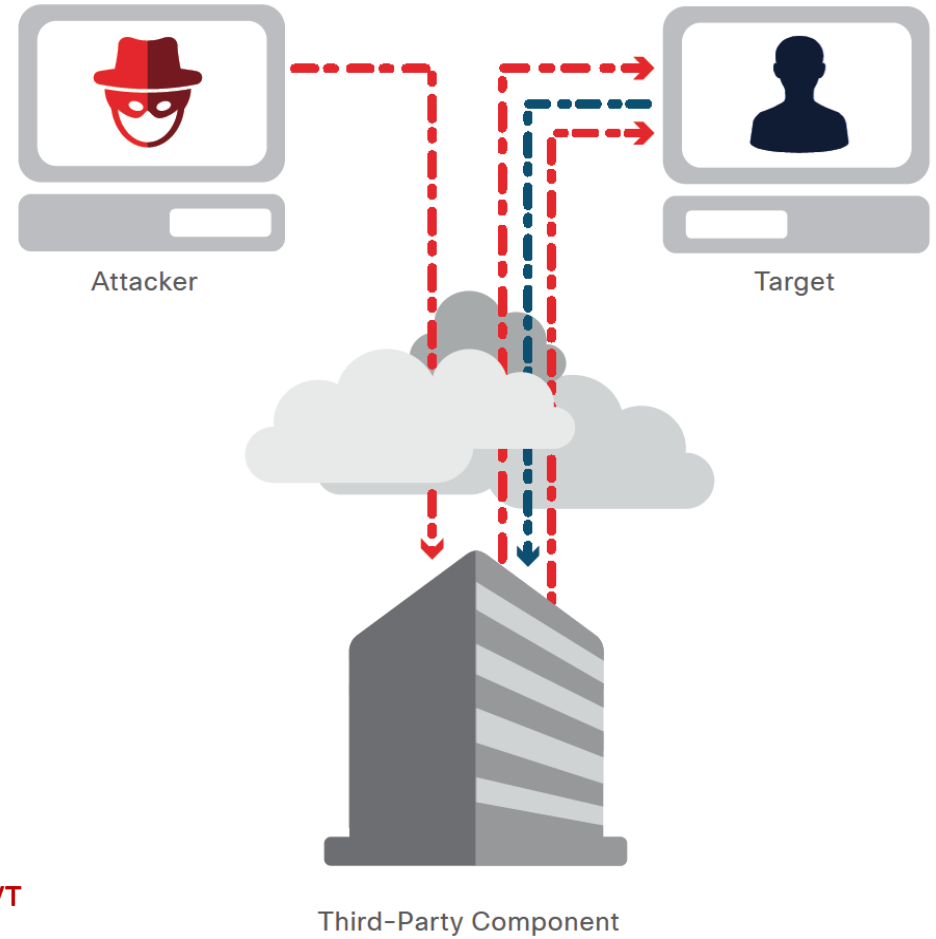
Cisco 2017 Midyear Cybersecurity Report: cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html

Сокращение длительности атак и отсутствие расследований по результатам воздействий

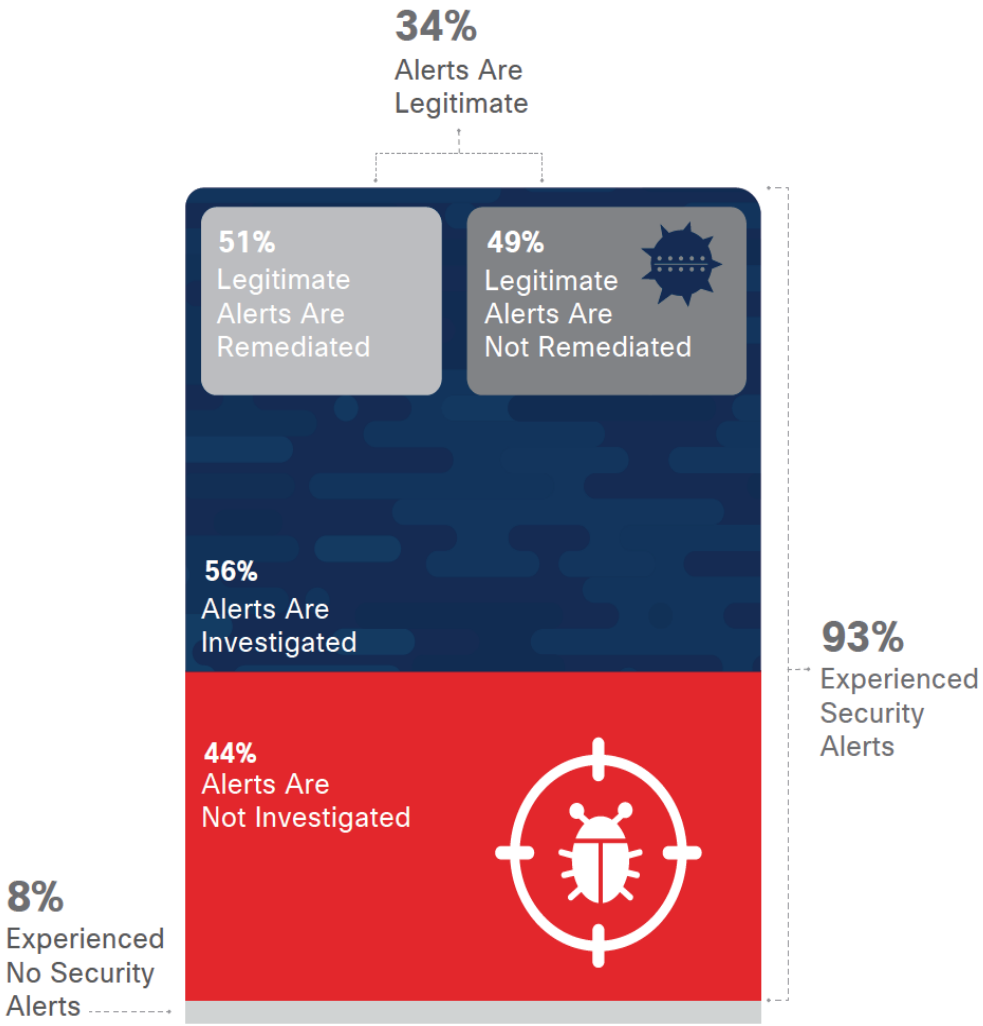
42% Experienced Short-Burst DDoS Attacks in 2017



Половина DDOS менее 30 минут



Атаки через промежуточные узлы



Половина воздействий не изучается

Cisco 2017 Midyear Cybersecurity Report: cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html

Типовые подходы к защите информации в РИТКС

Управление инцидентами кибербезопасности

Выявление внешних угроз и внутренних нарушителей, потенциально опасные действия персонала и ошибки конфигурации:

- сбор данных из различных источников;
- анализ сетевого трафика;
- построение цепочек атак;
- интеграция в деятельность спецподразделений инструкций и регламентов реагирования.

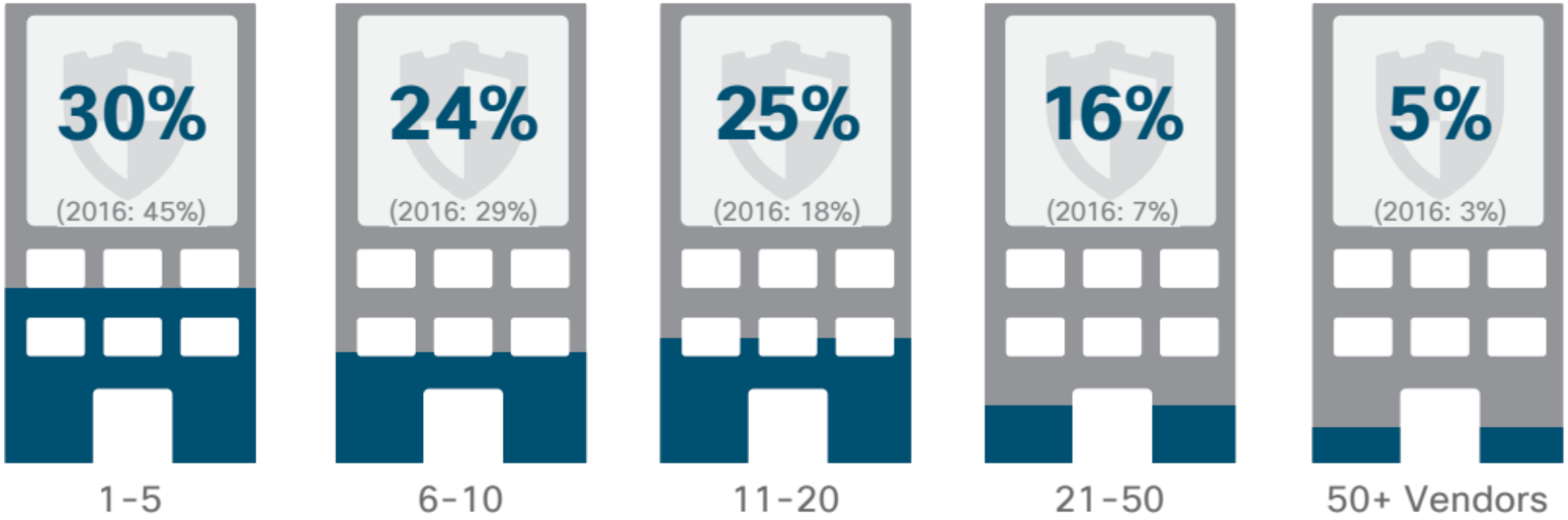
Анализ защищенности

Оценка состояния защищенности информационных систем, распределенных узлов ИТКС и приложений:

- тестирование на проникновение;
- системные проверки инфраструктуры;
- контроль соответствия политики безопасности;
- анализ ОС, СУБД, Web-приложений, внешних подключений.

Используемые вендоры

Количество производителей средств защиты информации, решения которых используются в организациях в 2018 году увеличилось



* Cisco 2018 Annual Cybersecurity report