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

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

CNews ФОРУМ 2017:
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ЗАВТРА

10 CNews FORUM 2017 2007-2017 лет

26 октября 2017 Президент России обозначил пять приоритетных направлений, по которым будет развиваться кибербезопасность в государстве

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.

2018-2020

Проект финансирования плана мероприятий по разделу «Информационная безопасность» программы «Цифровая экономика»

3 ДЕПАРТАМЕНТ СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ

КИБЕРБЕЗОПАСНОСТЬ РФ

Плановое финансирование 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 **интернет-вещей**	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

ФСТЭК России: угрозы и уязвимости

Уязвимости системного программного обеспечения

Уязвимости прикладного программного обеспечения

Уязвимости используемых телекоммуникационных протоколов

Стационарные аппаратно-программные комплексы

Мобильные платформы

Изменения в нормативной базе федерального уровня

Указ Президента	Указ Президента Российской Федерации от 05.12.2016 г. № 646 Об утверждении Доктрины информационной безопасности Российской Федерации
ФЗ	Федеральный Закон Российской Федерации «О безопасности критической информационной инфраструктуры Российской Федерации»
ПП РФ	Постановление Правительства РФ от 11.05.2017 №555 "О внесении изменений в требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации"
ПП РФ	Постановление Правительства РФ от 6 мая 2016 г. №399 «Об организации повышения квалификации специалистов по защите информации и должностных лиц, ответственных за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием и организациях ОПК»

Приказы ФСТЭК России

01.12.2015	Модель иностранных технических разведок до 2025 года (приказ)
09.02.2016	Требования к межсетевым экранам (приказ №9дсп)
16.04.2016	Требования по технической защите информации, содержащие сведения, составляющие ГТ (приказ)
19.08.2016	Требования безопасности информации к операционным системам (приказ №119)
19.08.2016	Требования к средствам уничтожения информации на машинных магнитных носителях информации способом магнитно-силового воздействия (приказ №18)
15.02.2017	Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (приказ №17)
23.03.2017	О внесении изменений в состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (приказ №49)

Информационные сообщения ФСТЭК России

2 июля 2017 240/22/3171	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
22 июня 2017 240/22/3031	О порядке рассмотрения и согласования моделей угроз безопасности информации и технических заданий на создание государственных информационных систем
18 октября 2016 240/24/4893	Об утверждении Требований безопасности информации к операционным системам
12 сентября 2016 240/24/4278	Об утверждении методических документов, содержащих профили защиты межсетевых экранов
20 июля 2016 240/24/3271	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 240/24/3246	Об уязвимостях в сертифицированных средствах защиты информации Dallas Lock 8.0
28 апреля 2016 240/24/1986	Об утверждении Требований к межсетевым экранам
12 апреля 2016 240/24/1649	Об уязвимостях в сертифицированных средствах защиты информации Secret Net и мерах по их нейтрализации

Анализ уязвимостей ФСБ России по ИТКС

Поиск уязвимостей в ИТКС и ИС

Повышение привилегий

Устаревшее ПО

VPN

- 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
- …

Появление новых видов целевых компьютерных атак

Advanced persistent threats (APT-атаки)

2016 год – год 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.

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

Современные наборы эксплойтов используют старые уязвимости

Reign of Ransomware 2016

По данным TrendMicro: с первого полугодия 2016 года количество программ-вымогателей выросло на 172%

Обновление вредоносных программ для PoS-терминалов

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

Течение APT-атаки

Подготовка	Проникновение	Распространение	Реализация цели
Получение информации	– Получены данные	– Тиражирование в системе	
Социальная инженерия	**Целевой фишинг**	**RAT**	**Кейлоггеры**
Фишинговые ссылки	**Эксплойты**	**Бэкдоры**	**Шпионы**
	Инсайдеры	**Самоуничтожение**	**Перехват**
	Уязвимости нулевого дня		
Извлечение конфиденциальных данных жертвы	Внедрение средства удаленного администрирования	Заражение и получение доступа к управлению данными	Реализация последующим управлением
– Подготовка	– Начало реализации	– Реализация	– Фоновый режим
	– Не завершена	– Получение данных	

СРЕДСТВО РЕАЛИЗАЦИИ

РЕЗУЛЬТАТ РЕАЛИЗАЦИИ

Современные DDOS-атаки

Автономные системы защиты

Защита на уровне провайдера

VOLUMETRIC ATTACKS

Отправка пакетов UDP/ICMP

TCP STATE-EXHAUSTION ATTACKS (PROTOCOL ATTACKS)

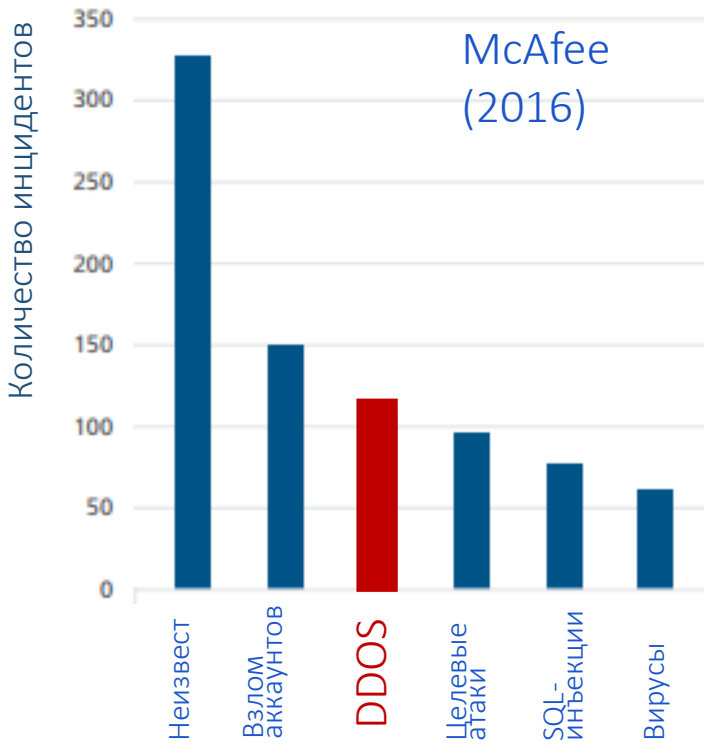
Используют в реализации уровень приложений

APPLICATION-LAYER ATTACKS

Используют в реализации прикладной уровень

ZERO-DAY DDOS ATTACKS

Используют ранее неизвестные уязвимости эксплойтов



Одноименная Dyn – атака была DDoS-атакой, использующей IoT-устройства как боты для атаки на DNS сервис провайдера. Пиковая ширина канала Dyn-атаки достигла 1.2 Тб/с.

Опасности IOT-устройств

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

Университет Твенте, Нидерланды

70%

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

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

Вычислительные мощности IoT-устройств (домашних роутеров) превышают профильные требования к данным устройствам

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

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.