Алексей Лукацкий
Chief Evangelist Officer

Формирование чеклиста с требованиями по ИБ к подрядчикам

И никаких «цепочек поставок»

Who am I?

- Бизнес-консультант по безопасности в Positive Technologies, Chief Evangelist Officer
- Автор проекта «Бизнес без опасности»
- Автор 5 книг и 30+ курсов по ИБ
- Программист, админ, аудитор, маркетолог, продавец, консультант, преподаватель, rCISO, писатель, популяризатор
- 30+ лет в кибербезе



Известные кейсы (часть)

- SolarWinds
- Codecov
- Kaseya
- ua-parser-js, node-ipc (и много других NPM)
- Библиотеки в PyPi
- ManageEngine ADSelfService Plus
- CocoaPods
- Passwordstate
- Okta
- 3CX
- CCleaner
- MOVEit
- Airbus
- Discord Bot
- JetBrains
- Jfrog Antifactory
- Norton
- ShadowHammer/ ASUS
- Applied Materials
- MeDoc (NotPetya)...



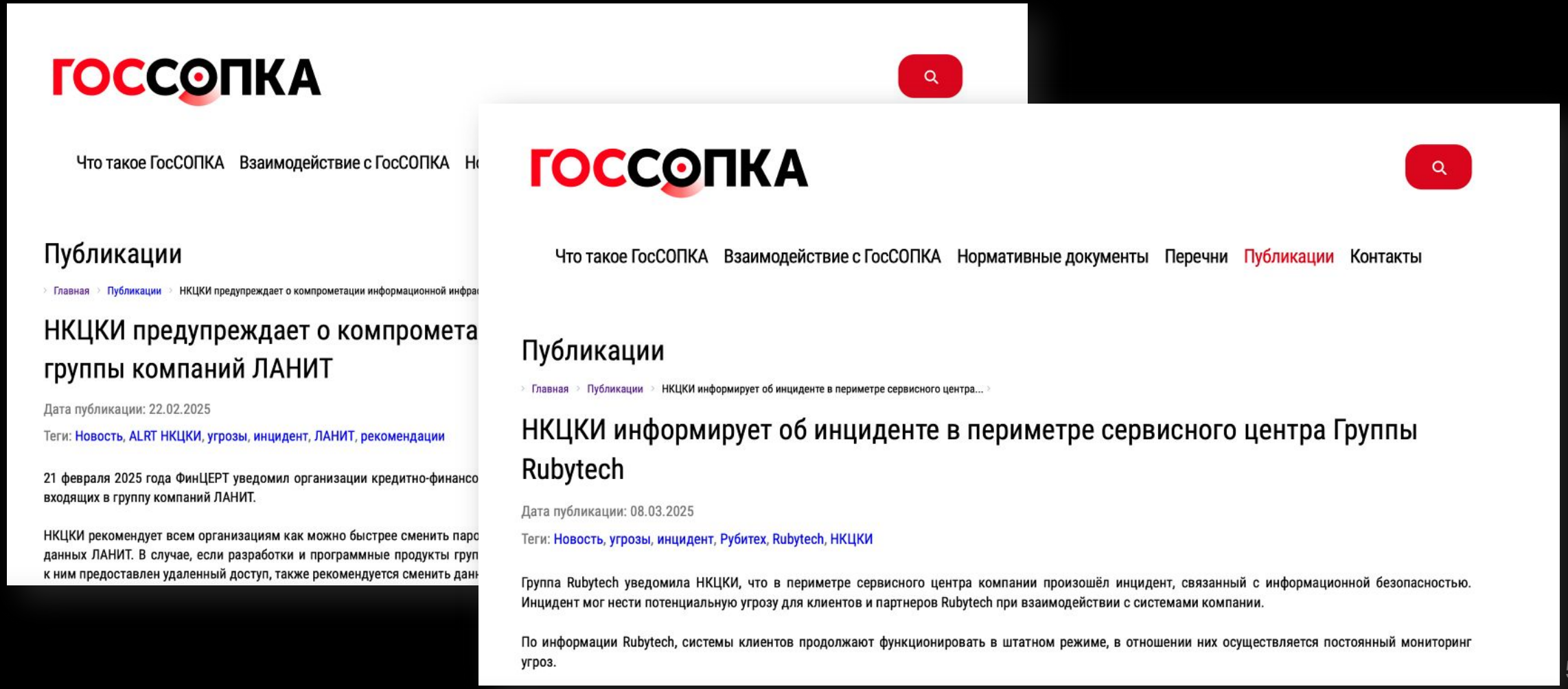
Известные кейсы в России

- Виджет Минэкономразвития, размещенный на сайтах многих министерств

И всё?!



Кейсы в РФ участились





Атаки на разработчиков ПО из России

Более 50 кейсов

Атаки на ИБ-компании из РФ



Как защищать(ся от) подрядчиков

1. Определение списка подрядчиков
2. Классификация и приоритизация
3. Моделирование угроз
4. Установление требований
5. Проверка реализации требований
6. Непрерывный мониторинг



Знай своего подрядчика

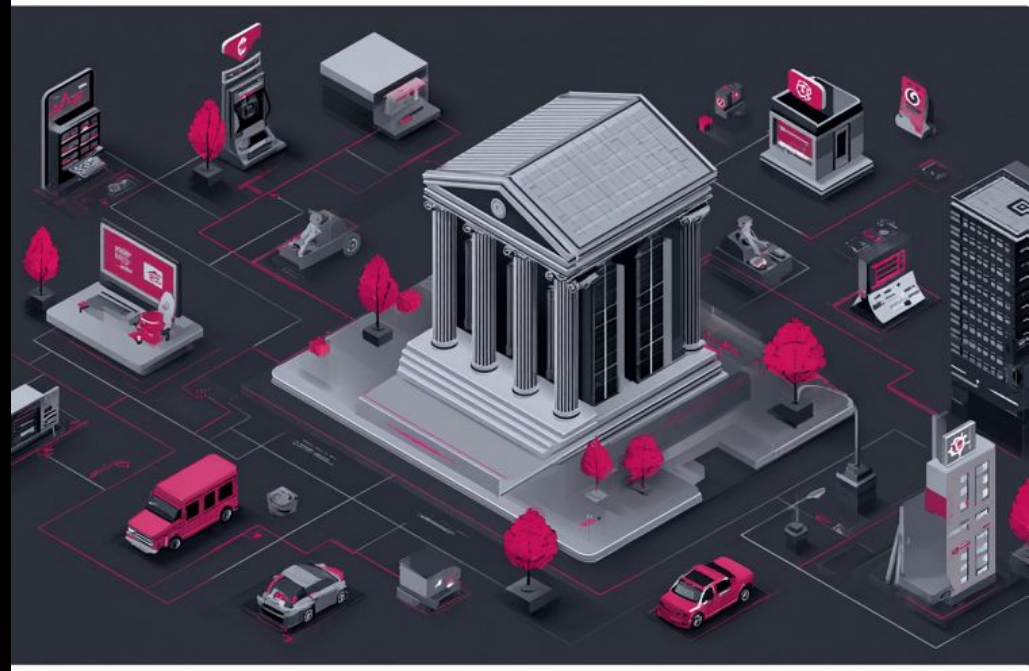
- Поставщики ПО и железа
- Разработчики используемых библиотек и компонентов
- Хостинг-провайдеры, операторы связи, регистраторы и DNS-сервисы
- Провайдеры MSP / MSSP / MDR / SOC
- ИТ/ОТ-интеграторы
- Поставщики электроэнергии
- Поставщики финансовых и иных услуг...



Подрядчики банка

- Финансовые услуги и партнёры по основному бизнесу
- ИТ-инфраструктура и цифровые сервисы
- Подрядчики по аппаратным и сервисным решениям
- Маркетинг, продажи и взаимодействие с клиентами
- Безопасность и контроль
- Операционная поддержка и управление персоналом
- Общие офисные и инфраструктурные подрядчики
- Юридические и консультационные услуги
- Дополнительно

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ КАТЕГОРИЙ ПОДРЯДЧИКОВ



ДЛЯ БАНКА

Фрагмент документа

Примерный перечень категорий подрядчиков

ФИНАНСОВЫЕ УСЛУГИ И ПАРТНЁРЫ ПО ОСНОВНОМУ БИЗНЕСУ

Процессинговые центры и платёжные системы
a. Visa, MasterCard, Мир и пр. (хоть и не «подрядчики» в классическом смысле, но важные партнёры).
b. Партнёры по эквайрингу для торговых точек.

Бюро кредитных историй (БКИ)
a. Кредитные рейтинги, проверка заёмщиков.

Страховые компании-партнёры
a. Продажа страховых продуктов через банк (например, страхование жизни при кредите).

Клиринговые и расчётные организации
a. Национальные/международные клиринговые системы для межбанковских расчётов.

Аутсорсинг коллекторских услуг
a. Сбор просроченной задолженности (при необходимости).

ПРЕДУПРЕЖДЕНИЕ

Этот список — примерная ориентировочная матрица возможных подрядчиков и партнёрских организаций, с которыми взаимодействует розничный банк.

В реальной практике перечень может варьироваться в зависимости от масштаба, внутренних ресурсов (часть услуг может быть «in-house») и сферы деятельности (международный банк или локальный).

ИТ-ИНФРАСТРУКТУРА И ЦИФРОВЫЕ СЕРВИСЫ

Дата-центры / хостинг-провайдеры
a. Физическое размещение серверов, аренда стоек, частные облака (Private Cloud), колокейшн.

Облачные провайдеры (IaaS, PaaS, SaaS)
a. AWS, Azure, Google Cloud, локальные облачные провайдеры.
b. Использование облака для внутренних сервисов, бэкапов, аналитики и т. п.

Провайдеры DNS и доменных имён
a. Компании, регистрирующие и обслуживающие домены банка.

Подрядчики банка

- Поставщики товаров и сырья
- Логистика и складская инфраструктура
- ИТ и цифровые решения
- Безопасность и контроль
- E-commerce и финансовые сервисы
- Оборудование для магазинов и техподдержка
- Юридические и консалтинговые услуги
- Маркетинг и продвижение
- Обслуживание торговых точек и офисов
- HR и аутсорсинг отдельных функций
- Общая логистика и управление инфраструктурой
- Дополнительно

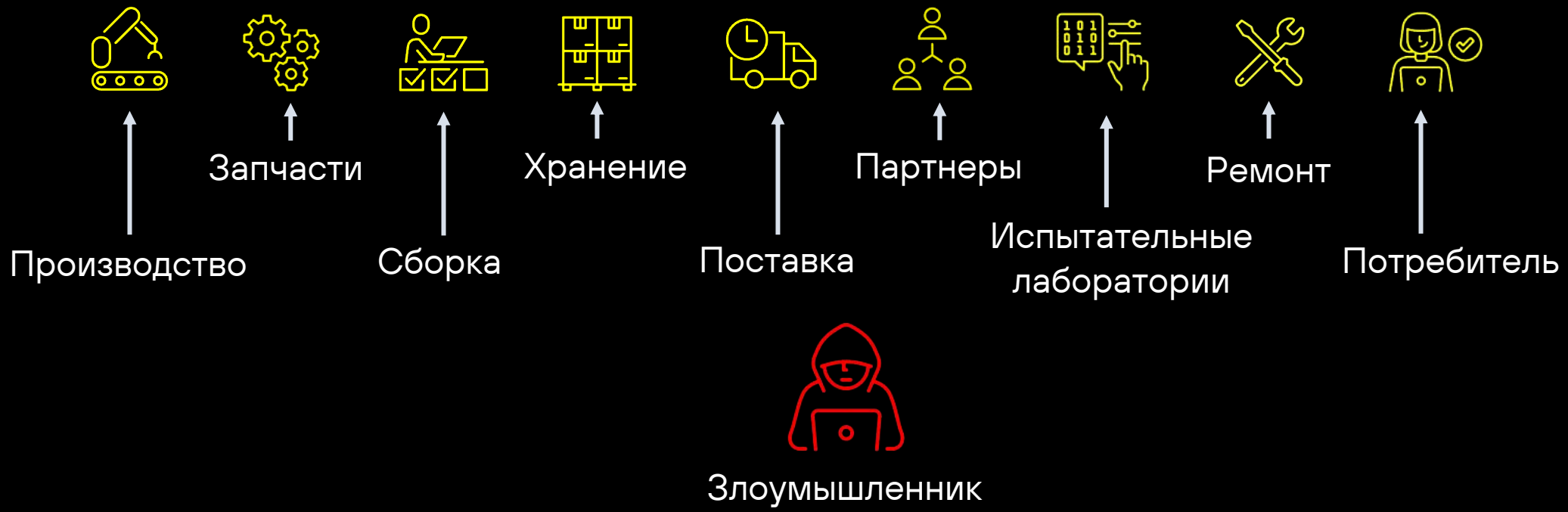
pt

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ КАТЕГОРИЙ ПОДРЯДЧИКОВ



ДЛЯ ПРЕДПРИЯТИЙ ИЗ СФЕРЫ РОЗНИЧНОЙ ТОРГОВЛИ

Смотрите на всю цепочку доставки продуктов / сервисов / запчастей



Процедура производства и поставки оборудования (пример)

Не все подрядчики одинаково полезны



Это вы!

Как найти всех?

- Анализ трафика на NGFW или SWG
- Анализ договоров (у юристов)
- Опрос подразделений





Не все одинаковы

- Какие услуги/работы переданы: ИТ-поддержка, разработка ПО, хранение данных, аутсорсинг некоторых бизнес-процессов и т.д.
- Какой уровень доступа есть у каждого подрядчика? (критичные системы, конфиденциальные данные и т.д.)

Приоритизируйте

- Размер дохода
- Доступ к важным/ценным данным
- Объем данных и число узлов, к которым подрядчик имеет доступ
- Может ли подрядчик стать причиной вашей компрометации или реализации недопустимого?
- Попробуйте Impact Analysis Tool for Interdependent Cyber Supply Chain Risks

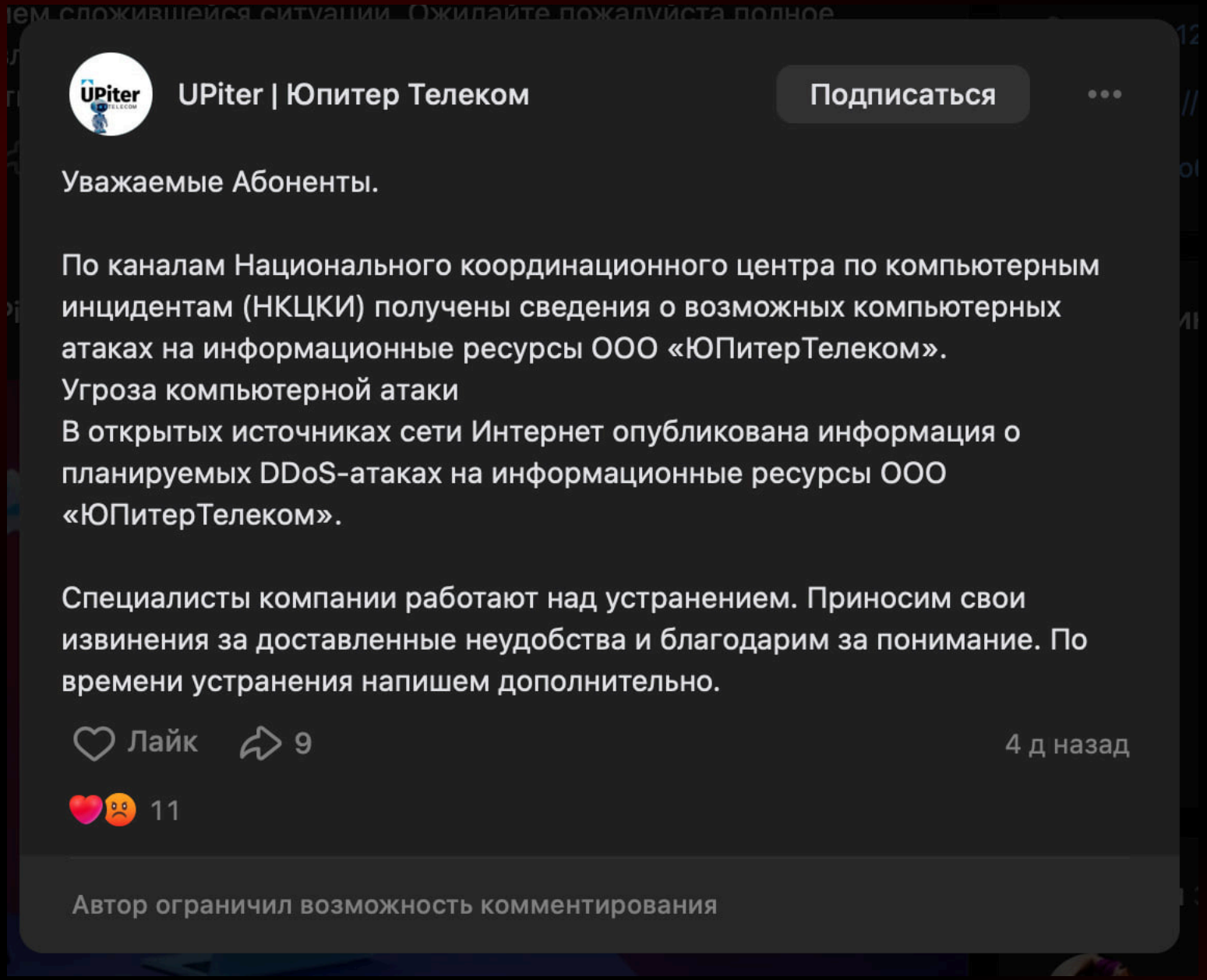


https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8272.pdf

Подход к классификации

- **Уровень доступа к конфиденциальным данным**: получают ли подрядчики доступ к персональным данным, финансовой информации, интеллектуальной собственности, критическим бизнес-процессам и т.д.
- **Степень интеграции в ИТ-инфраструктуру**: есть ли у подрядчика VPN-доступ, учётные записи в корпоративных системах, права администратора и т.д.
- **Влияние на непрерывность бизнеса**: если этот подрядчик перестанет работать или его взломают, насколько критично это отразится на операциях компании?
- **Регуляторные требования**: бывают ситуации (например, КИИ, PCI DSS, GDPR), где отдельные категории подрядчиков автоматически попадают в «высокий риск», если обрабатывают соответствующие данные





Доступность провайдеров

Уровень 1 - высокий риск

- Это подрядчики, которые:
  - Имеют доступ к наиболее важным или конфиденциальным данным (персональные данные клиентов, финансовые транзакции, коммерческая тайна)
  - Оказывают жизненно важные сервисы, без которых бизнес не может функционировать (поддержка ядра инфраструктуры, основная платёжная система и т.д.)
  - Подпадают под обязательные регуляторные требования (например, процессы, связанные с гособоронзаказом, PCI DSS, GDPR) и за их нарушения компания несёт высокую ответственность



Примеры 1-го уровня

DNS?

- ИТ-аутсорсинг / Managed Service Providers (MSP), которые поддерживают ключевые серверы, сети, базы данных
- Разработчики ПО, имеющие доступ к исходному коду основных продуктов компании или к производственному окружению (production)
- Провайдеры облачных решений (IaaS, PaaS, SaaS), где хранится или обрабатывается критичная информация (например, CRM с клиентскими данными)
- Платёжные шлюзы, эквайеры (если компания принимает онлайн-платежи), а также поставщики, связанные с обработкой платёжных карт (подтягиваются требования PCI DSS)
- Сервисы, обрабатывающие персональные данные (медицинские, финансовые, кадровые), объем которых попадает под оборотные штрафы

Github?



Требования для уровня

- Подробная проверка безопасности (аудит, анкетирование по приказам ФСТЭК, ГОСТ 57580, ISO/NIST/SIG, SOC 2, CSA, PCI DSS, CMMC и т.д.)
- Раз в год (или чаще) повторная оценка
- Обязательная формализация требований в SLA/контракте, право на аудит/пентест
- Жёсткий контроль доступа (VPN, MFA, мониторинг активности)



Уровень 2 – средний риск

- Это подрядчики, которые:
  - Могут иметь ограниченный доступ к системам или данным, но не к самым критичным
  - Влияют на бизнес, но сбой или взлом не парализуют компанию полностью
  - Не всегда подпадают под строгие регулятивные рамки, однако потенциальная утечка может иметь негативные последствия



Помните, что оборотные штрафы накладывают не за утечку?

Примеры 2-го уровня

- Маркетинговые агентства, получающие доступ к определённой части клиентской базы для проведения email-кампаний
- Хостинг провайдеры (не для критичных систем) или «обычные» SaaS-сервисы, в которых компания хранит не слишком чувствительные, но полезные данные (например, внутренние отчёты)
- Аутсорсинговые компании по разработке веб-сайтов (без доступа к основным боевым сервисам), тестовые среды
- Консалтинговые фирмы, получающие некоторую информацию о бизнес-процессах, но не работающие с «секретными» данными



Требования для уровня

- Стандартная проверка безопасности (анкетирование, возможно запрос базового отчёта о кибербезе)
- Подписание NDA и базовые условия в SLA по уведомлению об инцидентах
- Регулярная ревизия прав доступа
- Отчётность и предоставление подтверждающей документации (например, о прохождении внутреннего аудита)



Уровень 3 – низкий риск

- Это подрядчики, доступ или влияние которых на бизнес минимальны. Их взлом может быть неприятным, но не вызовет серьёзных потерь для компании
- Примеры:
  - Поставщики логистических услуг, если они не обрабатывают конфиденциальные данные, а только получают адреса отгрузки (обычные ПДн)
  - Уборка помещений или сервисы по обслуживанию офиса, не имеющие доступа к корпоративным системам (хотя могут быть физические риски доступа в помещения, но в общем случае это низкая критичность)
  - Партнёры по печати рекламных материалов, агентства наружной рекламы и т.п.
  - Технические подрядчики, которые занимаются, например, ремонтом офисного оборудования (если нет доступа к внутренней сети)



Требования для уровня

- Подписание NDA/обязательств о конфиденциальности (если требуется)
- Базовые организационные меры (не оставлять их без сопровождения в критичных зонах, контролировать физический доступ)
- Обычно не требуется глубокой проверки ИБ, но компания может иметь форму опросника «минимальных» требований (например, наличие антивируса /EDR лучше/, базовые политики паролей...)



Уровень 0

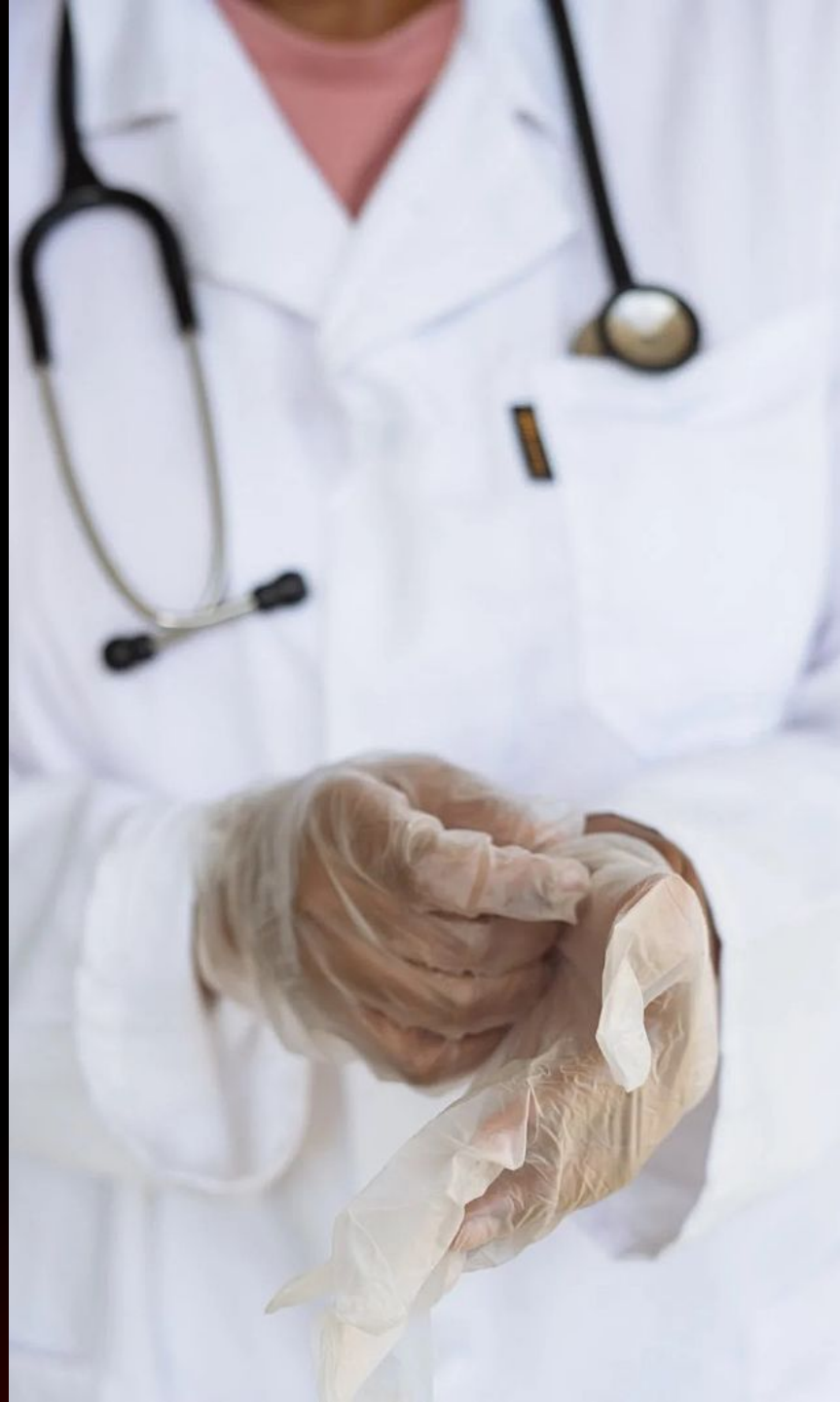
- Иногда выделяют 4 уровня, добавляя «экстракритичный» (или нулевой), если подрядчик фактически является частью бизнеса (например, полностью ведёт DevOps или хранит ключевую базу данных)
- Могут быть специализированные категории:
  - Разработчики ПО с доступом к репозиториям → идут в высокий риск, даже если формально они «маленькие» поставщики
  - Сотрудники колл-центра на аутсорсе → если обрабатывают много клиентских данных, тоже повышают категорию риска
  - Инсорсеры в группе компаний – кто они для вас?



Важные вопросы

- У вас проведена инвентаризация всех своих активов?
- Что делать с субподрядчиками?
- Что, если ваши подрядчики не готовы к дополнительным требованиям по кибербезопасности?

Готовы отказаться от них?





Чего мы боимся?

- Внедрение программных закладок
- Подмена программных компонентов
- Компрометация системы удаленного управления
- Компрометация сайтов подрядчиков
- Аппаратные импланты
- Подмена аппаратных компонентов
- НСД со стороны сотрудников подрядчика
- Нарушение доступности
- Что-то еще?..

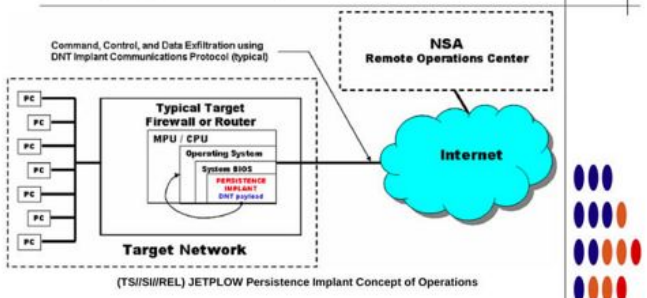
Какова ваша модель нарушителя?

TOP SECRET//COMINT//REL TO USA, FVEY

JETPLOW
ANT Product Data

(TS//SI//REL) JETPLOW is a firmware persistence implant for Cisco PIX Series and ASA (Adaptive Security Appliance) firewalls. It persists DNT's BANANAGLEE software implant. JETPLOW also has a persistent back-door capability.

06/24/08



(TS//SI//REL) JETPLOW Persistence Implant Concept of Operations

(TS//SI//REL) JETPLOW is a firmware persistence implant for Cisco PIX Series and ASA (Adaptive Security Appliance) firewalls. It persists DNT's BANANAGLEE software implant and modifies the Cisco firewall's operating system (OS) at boot time. If BANANAGLEE support is not available for the booting operating system, it can install a Persistent Backdoor (PBD) designed to work with BANANAGLEE's communications structure, so that full access can be reacquired at a later time. JETPLOW works on Cisco's 500-series PIX firewalls, as well as most ASA firewalls (5505, 5510, 5520, 5540, 5550).

(TS//SI//REL) A typical JETPLOW deployment on a target firewall with an exfiltration path to the Remote Operations Center (ROC) is shown above. JETPLOW is remotely upgradeable and is also remotely installable provided BANANAGLEE is already on the firewall of interest.

Status: (C//REL) Released. Has been widely deployed. Current availability restricted based on OS version (inquire for details).

Unit Cost: $0

POC: [redacted], S32222, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

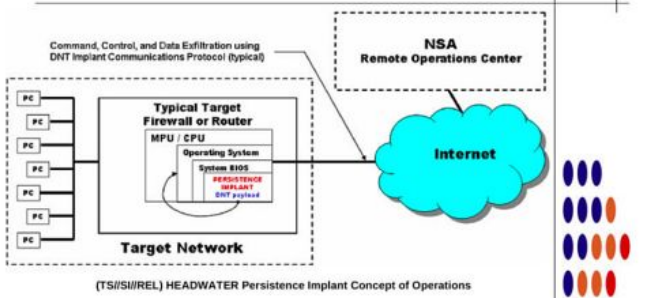
TOP SECRET//COMINT//REL TO USA, FVEY

TOP SECRET//COMINT//REL TO USA, FVEY

HEADWATER
ANT Product Data

(TS//SI//REL) HEADWATER is a Persistent Backdoor (PBD) software implant for selected Huawei routers. The implant will enable covert functions to be remotely executed within the router via an Internet connection.

06/24/08



(TS//SI//REL) HEADWATER Persistence Implant Concept of Operations

(TS//SI//REL) HEADWATER PBD implant will be transferred remotely over the Internet to the selected target router by Remote Operations Center (ROC) personnel. After the transfer process is complete, the PBD will be installed in the router's boot ROM via an upgrade command. The PBD will then be activated after a system reboot. Once activated, the ROC operators will be able to use DNT's HAMMERMILL Insertion Tool (HIT) to control the PBD as it captures and examines all IP packets passing through the host router.

(TS//SI//REL) HEADWATER is the cover term for the PBD for Huawei Technologies routers. PBD has been adopted for use in the joint NSA/CIA effort to exploit Huawei network equipment. (The cover name for this joint project is TURBOPANDA.)

Status: (U//FOUO) On the shelf ready for deployment.

POC: [redacted], S32222, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

TOP SECRET//COMINT//NOFORN

June 2010

SID today

(U) Stealthy Techniques Can Crack Some of SIGINT's Hardest Targets

By: (U//FOUO) [redacted], Chief, Access and Target Development (S3261)



(TS//SI//NF) Not all SIGINT tradecraft involves accessing signals and networks from thousands of miles away… In fact, sometimes it is very hands-on (literally!). Here's how it works: shipments of computer network devices (servers, routers, etc.) being delivered to our targets throughout the world are ***intercepted***. Next, they are ***redirected to a secret location*** where Tailored Access Operations/Access Operations (AO – S326) employees, with the support of the Remote Operations Center (S321), enable the ***installation of beacon implants*** directly into our targets' electronic devices. These devices are then re-packaged and ***placed back into transit*** to the original destination. All of this happens with the support of Intelligence Community partners and the technical wizards in TAO.

(TS//SI//NF) Such operations involving **supply-chain interdiction** are some of the most productive operations in TAO, because they pre-position access points into hard target networks around the world.



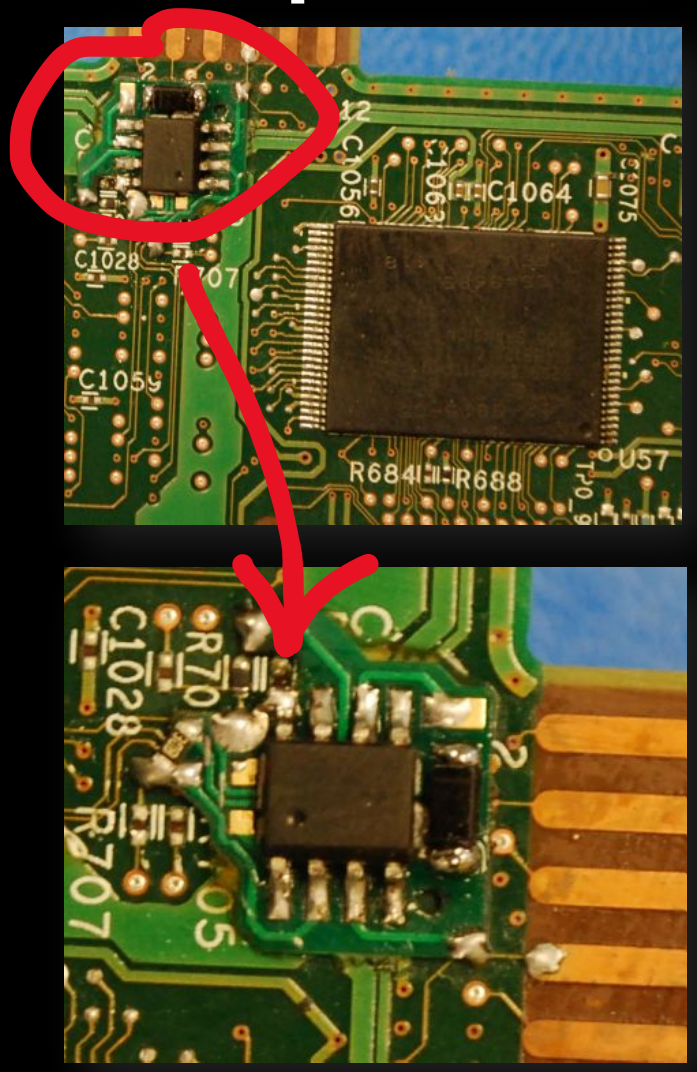
(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

(TS//SI//NF) In one recent case, after several months a beacon implanted through supply-chain interdiction called back to the NSA covert infrastructure. This call back provided us access to further exploit the device and survey the network. Upon initiating the survey, SIGINT analysts from TAO/Requirements & Targeting determined that the implanted device was providing even greater accesses than we had hoped: We knew the devices were bound for the Syrian Telecommunications Establishment (STE) to be used as part of their internet backbone, but what we did not know was that STE's GSM (cellular)

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20350501

TOP SECRET//COMINT//NOFORN

Не все можно легко обнаружить
Аппаратные импланты



- Установка дополнительного чипа и микроконтроллера на плате маршрутизатора Cisco
  - Выполнение расширенного функционала
- Внедрение вредоносного ПО в память маршрутизатора
  - Обход лицензионных проверок
  - Возможность работы дополнительного чипа

Моделирование угроз

- Запросите модель угроз у подрядчика
  - Помните, что это требует и ФСТЭК в своей методике оценки угроз
- Проанализируйте модель и сопоставьте со своей моделью угроз
  - У вас же есть своя модель? :-)
- При отсутствии, разработайте раздел в свою модель угроз



Как мы ловим угрозы?

Это важно для мониторинга!

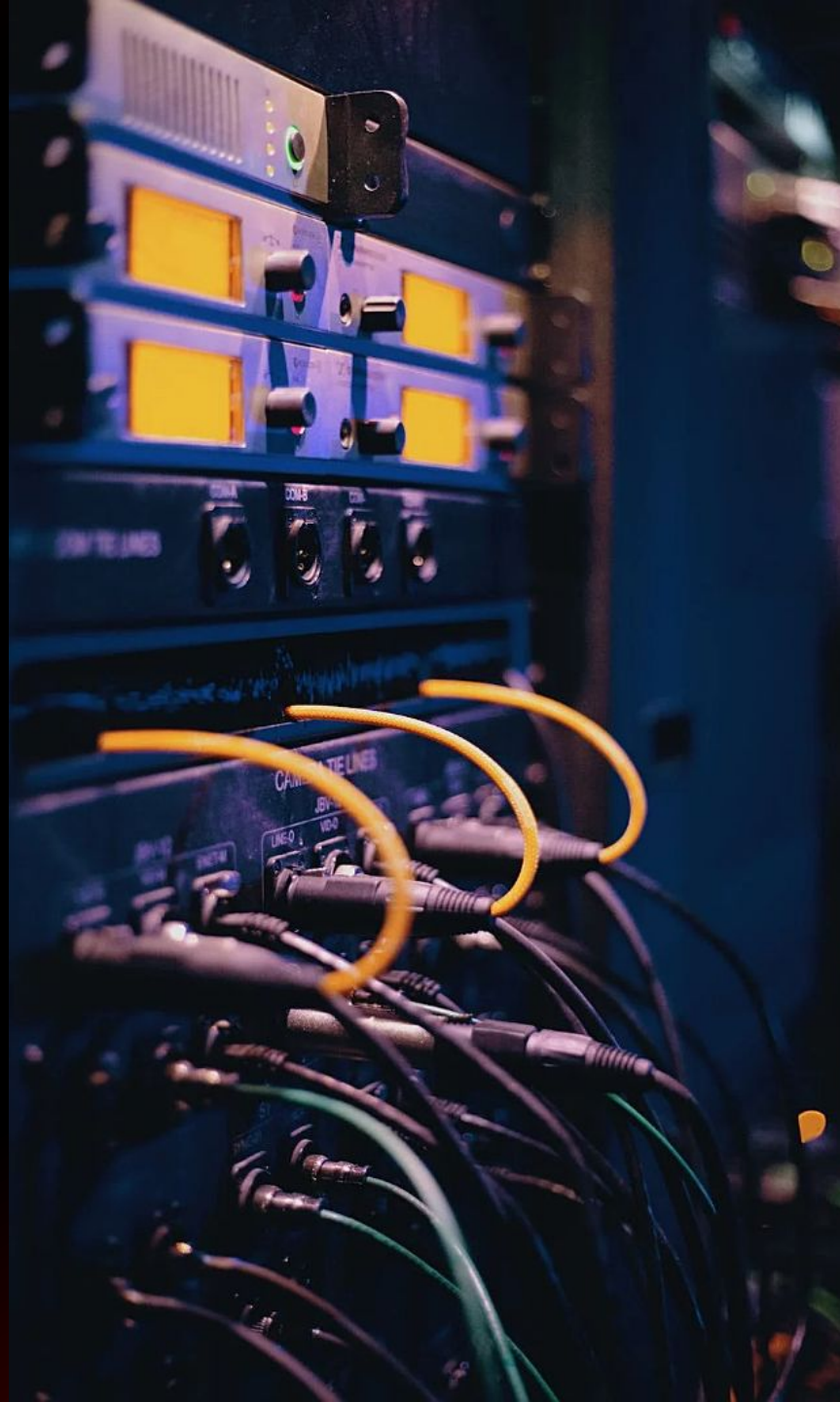


Индикаторы

- Файловые (хеши и имена файлов)
- Сетевые (IP, имена доменов)
- Поведенческие (нетипичный трафик или системная активность)
- Артефакты (ключи реестра, конфиги, сертификаты)

Сетевые индикаторы

- Нетипичный трафик в сторону подрядчика или от него
- Превышение типичного объема данных
- ПО подрядчика коммуницирует с известными C2-серверами или нетипичными IP / доменами / геолокациями
- Сканирование со стороны подрядчика



TLS fingerprinting



- Обнаружение аномалий по отпечатку клиентского ПО в сетевом трафике (TLS + хеши JA3/JA3S)
  - Выявление JA3 хэшей, характерных для популярных ПО и сетевых библиотек языков программирования
  - Выявление конкретного ВПО по хэшам JA3\JA3S
  - Выявления нового хэша JA3, ранее непоявляющегося в сети
  - Выявления хэшей JA3 не из белого списка
  - Выявления хэшей JA3\JA3S из черного списка
  - Выявление JA3 хэшей, не характерных для системы

Это open source'ная история!



Поведенческие индикаторы

- Доступ к нетипичным узлам или данным в инфраструктуре
- Повышение привилегий
- Доступ в нетипичное время
- Неудачные попытки аутентификации
- Нетипичные места входа

Файловые индикаторы

- Несоответствие хеша скачанного / полученного файла эталонному
- Неизвестные ранее файлы





Что типично для подрядчика?!

Что является предметом договора?

Каталог шаблонов атак

Attack Identifier: A3

Target (Attack Type): Hardware: Firmware:

Software: Yes

Description (Attack Act): System is compromised by the components during development or update.

Attack Vector: Adversary with access to software proce environment or software support activity update enviro

Attack Origin: Staff within the software engineering en

Attack Goal: Disruption: Yes

Corruption: Yes

Attack Impact: System may function in a manner that i

References: Based on NIST SP 800-30; page E-4

Threat: An adversary with access to software processes software support environment can insert malicious soft development or update/maintenance.

Vulnerabilities: The development environment or softv susceptible To an adversary inserting malicious softwar or update.

Attack Points: Program Office:

Prime Contractor: Yes

Sub-Contractor: Yes

Integrator Facility: Yes

Applicable Life Cycle Phases: Ma

Te

Engineering and Manufactur

Production

Opera

Шаблон атаки (один из 41)

Attack ID	Program Office	Prime Contractor	Sub-Contractor	Integrator Facility	SW Developer	HW Developer	SC Physical Flow	SC Info/Data Flow
A14	■							
A7	■	■						
A30	■	■						■
A37	■	■						■
A36	■	■		■				■
A28	■					■		
A16	■							■
A17	■							■
A13		■	■		■			
A18		■	■		■			
A3		■	■	■	■			
A4		■	■	■	■			
A40		■	■	■	■			
A41		■	■	■		■		
A20		■	■	■	■			■
A21		■	■	■	■			
A38		■	■	■	■			■
A39		■	■	■	■			■
A12		■	■	■	■	■	■	
A1		■	■	■	■		■	■
A8			■	■		■	■	
A9			■	■		■		
A23				■				
A19				■	■			
A26				■	■			
A32				■	■			
A10				■		■		
A25				■		■		
A5				■		■	■	
A29				■		■	■	
A31				■		■		■
A35					■		■	■
A6						■		
A22						■		
A24						■		
A33						■	■	
A34						■		
A2							■	
A11							■	
A15							■	
A27								■

Применимость атак



https://www.mitre.org/sites/default/files/publications/supply-chain-attack-framework-14-0228.pdf

Threat Intelligence

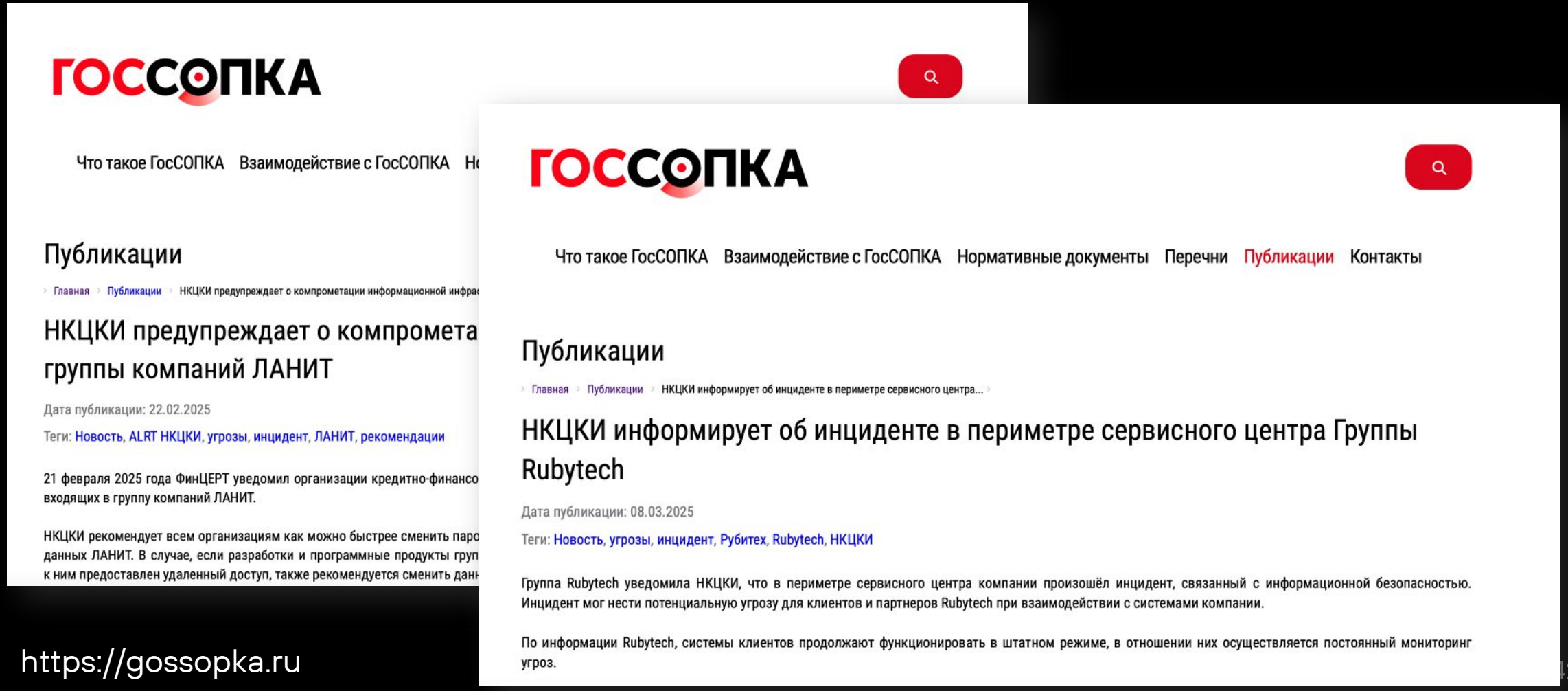


- Мониторинг источников TI с информацией об угрозах на подрядчиков

Organization	Breach Date	Adversary	Source
Boeing	November 2023	LockBit	cisa.gov / (archived)
BeyondTrust	October 2023	Unknown	beyondtrust.com / (archived)
Okta	October 2023	Unknown	sec.okta.com / (archived)
BHI Energy	October 2023	Akira	documentcloud.org / (archived)
D-Link	October 2023	"succumb"	dlink.com / (archived)
Kroll	August 2023	Unknown	kroll.com / (archived)
Microsoft	July 2023	Storm-0558 (CN MSS)	microsoft.com / (archived)
JumpCloud	July 2023	UNC4899 (DPRK RGB)	jumpcloud.com / (archived)
Dragos	May 2023	"KyivWarrior"	dragos.com / (archived)
3CX	March 2023	UNC4736 (DPRK RGB)	mandiant.com / (archived)
Coinbase	February 2023	0ktapus (suspected)	coinbase.com / (archived)
Reddit	February 2023	0ktapus (suspected)	reddit.com / (archived)
CircleCI	January 2023	Unknown	circleci.com / (archived)
LastPass	October 2022	Unknown	blog.lastpass.com / (archived)
Uber	September 2022	Lapsus$ (suspected)	uber.com / (archived)
Okta	August 2022	0ktapus	sec.okta.com / (archived)

https://github.com/BushidoUK/Breach-Report-Collection

Реактивно - рассылки ГосСОПКА



https://gossopka.ru



Базы данных уязвимостей

- Мониторинг известных уязвимостей в open source с помощью сканеров, фидов



https://osv.dev/

Проактивно – сюрвейинг by Positive Technologies

Сюрвейинг – это комплексная услуга по оценке устойчивости к кибератакам организаций, определенных по запросу заказчика.

Услуга в **базовом варианте** состоит из **4 этапов**:

- Анализ процессов и систем, связанных с защитой данных и ИТ-инфраструктурой оцениваемой организации (анкетирование).
- Экспресс сканирование внешнего сетевого периметра оцениваемой организации.
- Анализ публично-доступной информации об оцениваемой организации (киберпогоду).
- Ретроспективный анализ событий ИБ с ключевых компонентов ИТ-инфраструктуры оцениваемой организации.

Отчет по результатам сюрвейинга включает:

- Общий уровень устойчивости организации к кибератакам
- Потенциальные вектора атаки на организацию
- Подтверждение наличия или отсутствия:
  - уязвимостей внешнего сетевого периметра организации
  - индикаторов компрометации ИТ-инфраструктуры или подозрительных событий ИБ
  - утечек данных
  - фишинговых доменов
- Детали по обнаруженным недостаткам безопасности
- Рекомендации по повышению кибербезопасности

По завершении базового сюрвейинга может быть проведена дополнительная расширенная оценка с использованием других продуктов и сервисов Positive Technologies - PT Knocking, PT Dephaze, сервис по анализу конфигураций компонентов ИТ-инфраструктуры (ХардкорИТ) или другие предложения в зависимости от запроса заказчика.

Стоимость сюрвейинга зависит от размера инфраструктуры оцениваемой организации, а также включенных в сюрвейинг этапов оценки.

Средний срок оценки, включая подготовку отчета - 2 недели.



Независимо от того, кто проведет анализ подрядчиков, защищать вам!



Формализуем требования для подрядчиков

- Идем сверху вниз – от общего к частному

Рекомендации по созданию чеклиста



- Формализуйте ожидания и роли
  - Определите, какие именно объёмы данных и сервисы подрядчик обрабатывает, и подберите соответствующие стандарты (ФСТЭК, Банк России, ISO, NIST, PCI DSS и т. д.)
  - Пропишите обязательность соблюдения тех или иных норм и регламентов, включая обязанности по кибербезопасности, аудитам и уведомлениям об инцидентах
- Уточняйте соответствие регуляторным требованиям
  - Если подрядчик обрабатывает персональные данные, ему может быть необходимо соблюдать ФЗ-152 или местные законы (GDPR в Европе и т. д.)
  - Для финансовых компаний может быть важно соответствие PCI DSS, требованиям ЦБ и т. д.

В конце презентации будет подборка стандартов!

Рекомендации по созданию чеклиста



- Технические меры защиты на границе взаимодействия
  - Контроль доступа, шифрование, разделение сетей/сегментов для подрядчиков
  - Регулярный мониторинг действий подрядчиков в системах
- Непрерывный мониторинг и аудит
  - Раз в год (или иной периодичности) повторно оценивать риски поставщика
  - Учитывать любые изменения (например, M&A, изменение инфраструктуры и т. д.)
- План реагирования на инциденты (Incident Response)
  - Пропишите, как подрядчик обязан сообщать об инцидентах, в какие сроки и в каком формате
  - Определите совместные действия на случай, если у подрядчика случился взлом или утечка данных, найдена уязвимость или зафиксирована DDoS-атака

Не забывайте про взаимодействие с государственными организациями (ЕСИА, ЕБС, ГИС ГМП...)!

Рекомендации по созданию чеклиста



- Проводите регулярные аудиты и запросы на подтверждение
  - Запрашивайте аттестаты и сертификаты соответствия (ГОСТ, ФСТЭК, ISO 27001, PCI DSS и т. д.)
  - Используйте стандартизованные анкеты (SIG, CSA CAIQ) или собственную анкету с учётом отраслевых особенностей
  - Оценивайте подрядчиков повторно с установленной периодичностью (год, полгода) или после существенных изменений
- Включайте в контракты и SLA условия по информационной безопасности
  - Прописывайте ответственность сторон и санкции за нарушения
  - Требуйте уведомления при инцидентах и фиксируйте сроки реагирования

Это все и ФСТЭК будет требует в 117-м приказе!



Не забудьте!

- Определить уровень критичности подрядчика, данные и процессы, к которым он получает доступ
- Подбирать глубину проверок и требуемые меры на основе этой критичности
- Запрашивать подтверждения (сертификаты, отчёты аудиторов, результаты пентестов и т. д.)

3 группы требований

- Организационные требования
  - Наличие информационной (или кибер) безопасности как отдельной функции у подрядчика: кто отвечает за неё и какие политики есть?
  - Сертификация/аудит: 57580 (финансовые сервисы), ФЗ-152 (персданные), ISO 27001, PCI DSS, TISAX (автомобильная отрасль) и др.
  - Регулярная отчётность об инцидентах, уведомление об обнаруженных уязвимостях
  - Политика обучения персонала подрядчика (обязательно ли?)



3 группы требований

- Технические требования
  - Управление доступом: строгое разграничение прав, принцип наименьших привилегий, использование MFA
  - Шифрование данных: как при хранении, так и при передаче
  - Проверка кода (если это разработчики ПО): SAST, DAST, SBOM (Software Bill of Materials), SLSA-уровни сборки
  - Специсследования / спецпроверки (если это производитель / поставщик «железа») и HBOM
  - Мониторинг и логирование: какие логи должна предоставлять сторонняя организация, в каком формате, с какой периодичностью



3 группы требований

- Контрактные и юридические аспекты
  - Включение требований по безопасности в договоры (SLA, допсоглашения)
  - Ответственность подрядчика при утечке данных или при несоответствии требованиям
  - Чёткие сроки уведомления о любых инцидентах
  - Возможность аудита и пентестов (включая внезапные)





Детализируем требования для подрядчиков

- Могут уточняться и детализироваться в зависимости от ситуации

https://github.com/BushidoUK/Breach-Report-Collection

Топ10 мер

- Защита конфиденциальной информации и NDA
  - Подрядчик обязуется не разглашать сведения, полученные в ходе сотрудничества, и подписывает соглашение о неразглашении (NDA)
  - Гарантируется сохранение коммерческой тайны, персональных данных клиентов и работников, а также иных видов тайн
- Требования к системе управления безопасностью
  - Подрядчик подтверждает, что у него внедрены политики безопасности (например, основанные на приказах ФСТЭК, ISO 27001, SOC 2, NIST или другом стандарте) и что сотрудники проходят регулярное обучение
  - Может потребоваться предоставлять доказательства (сертификаты или аудиторские отчёты)
- Управление доступом и разграничение прав
  - Прописать принцип минимума привилегий: доступ только к тем данным и системам, что нужны для выполнения работ
  - Обязательная многофакторная аутентификация (MFA) к критичным системам (если актуально)
  - Регулярный пересмотр (ревизия) учётных записей



Топ10 мер

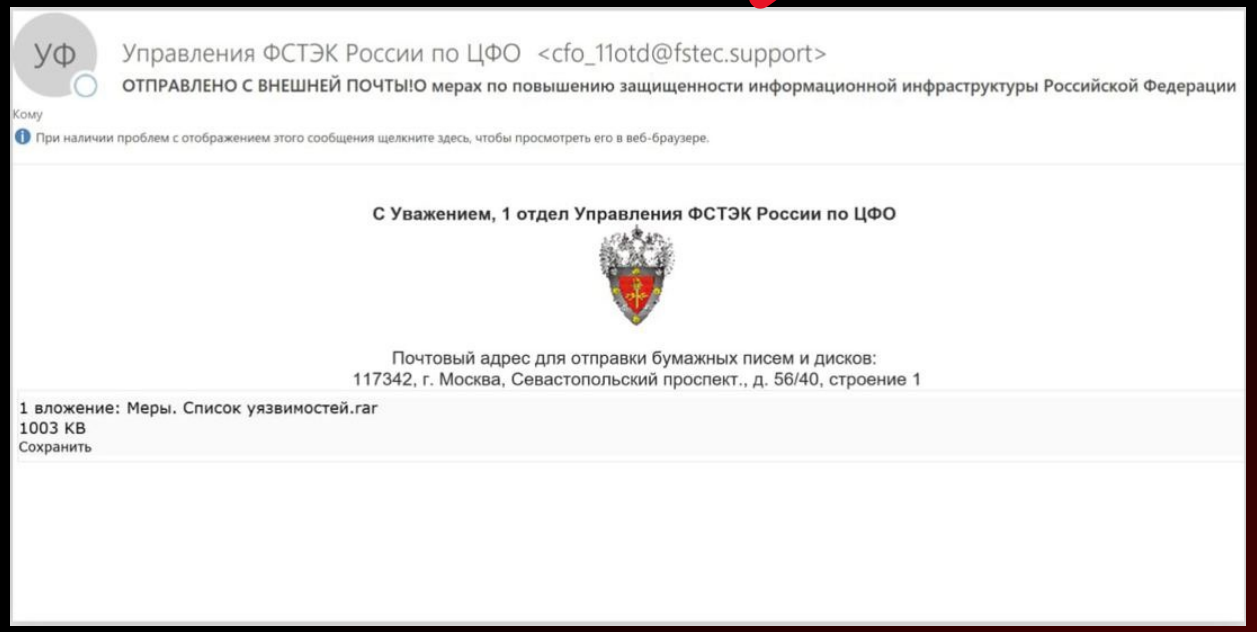
- Безопасная обработка и хранение данных
  - Чётко указать, какие данные обрабатываются и как они защищаются (шифрование при хранении и при передаче, резервное копирование, логи доступа)
  - Отдельно указать географические ограничения (если важно соблюдение GDPR или локальных законов)
- Уведомление об инцидентах в заданные сроки
  - Подрядчик обязан оперативно (например, в течение 24 часов) сообщать о любых инцидентах, утечках, взломах, связанных с данными или инфраструктурой заказчика
  - Описать формат и канал уведомления (e-mail, горячая линия), а также дальнейшие шаги
- Право на аудит и проверки
  - Заказчик может проводить (или нанимать третью сторону для проведения) аудит безопасности, в том числе внезапный/внеплановый, с разумными ограничениями (включая пентесты и кибериспытания)
  - Подрядчик обязан предоставлять доступ к нужным документам и системам в рамках аудита



Регуляторы – это тоже подрядчики

1.6. Ограничить возможность получения электронной почты с адреса postin@fstek[.]ru Обеспечить на уровне сетевых средств защиты информации

Вы знаете, какой домен верный – fstec.ru или fstek.ru?



Топ10 мер

- Управление изменениями (Change Management)
  - Подрядчик должен уведомлять заказчика о существенных изменениях (инфраструктура, команда, передача задач субподрядчикам) и согласовывать их, если они затрагивают уровень безопасности
  - Это предотвращает «резкие» изменения, которые могут открыть новые уязвимости
- Использование субподрядчиков
  - Запрет или ограничение на передачу работ субподрядчикам без согласия заказчика
  - Если субподрядчики привлекаются, на них тоже распространяются все пункты данного соглашения и аналогичные проверки



Топ10 мер

- План обеспечения непрерывности (BCP/DR) и реагирования на инциденты
  - Подрядчик подтверждает, что у него есть план действий в случае аварий или катастрофы, а также процедуры восстановления данных и систем
  - Должны быть описаны сроки восстановления и ответственные лица
- Условия завершения сотрудничества
  - Описать, как подрядчик обязан уничтожить или вернуть все полученные данные при расторжении договора (включая бэкапы, логи и т.д.)
  - Порядок отзыва доступов из систем, аннулирование учётных записей, ревизия ключей/сертификатов/токенов доступа



Особенности реализации

- Защита конфиденциальной информации и NDA
  - Регистрация: Вести реестр всех подписанных NDA и отслеживать, кто из сотрудников подрядчика (особенно тех, кто имеет прямой доступ к данным) действительно подписал документы
  - Обучение: Проверять, проводит ли подрядчик обучение сотрудников по политике конфиденциальности (можно запрашивать копии учебных материалов, отчёты о прохождении тренингов)
  - Мониторинг утечек: Системы DLP (Data Loss Prevention), мониторинг корпоративных e-mail, чатов (при необходимости и по взаимному согласию) — отслеживать, не утекают ли данные за периметр



Особенности реализации

- Требования к системе управления безопасностью (СУИБ)
  - Запрос сертификатов и отчётов: Попросить у подрядчика копию сертификата/аттестата (ISO 27001, SOC 2 и т. п.) и ежегодно запрашивать подтверждение актуальности. При необходимости — отчёт аудитора
  - Проверка соответствия: Сопоставлять практику подрядчика (по чек-листам и анкетам) с требованиями ISO/NIST/ГОСТ/17/21/239 и т.д.
  - Интервью или on-site аудит: Если риск высокий, провести выездную проверку (или видеоконференцию), где подрядчик показывает основные процессы управления безопасностью (политики, регистры рисков/НС, план действий)

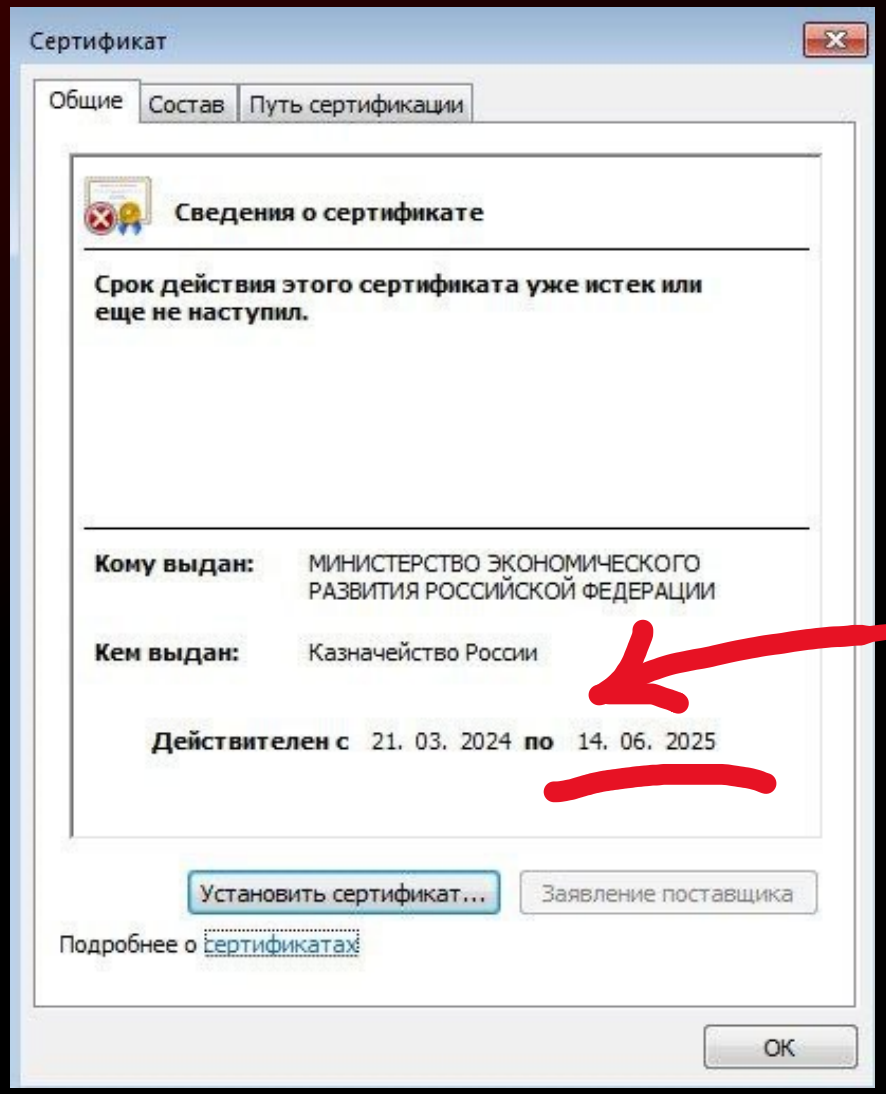


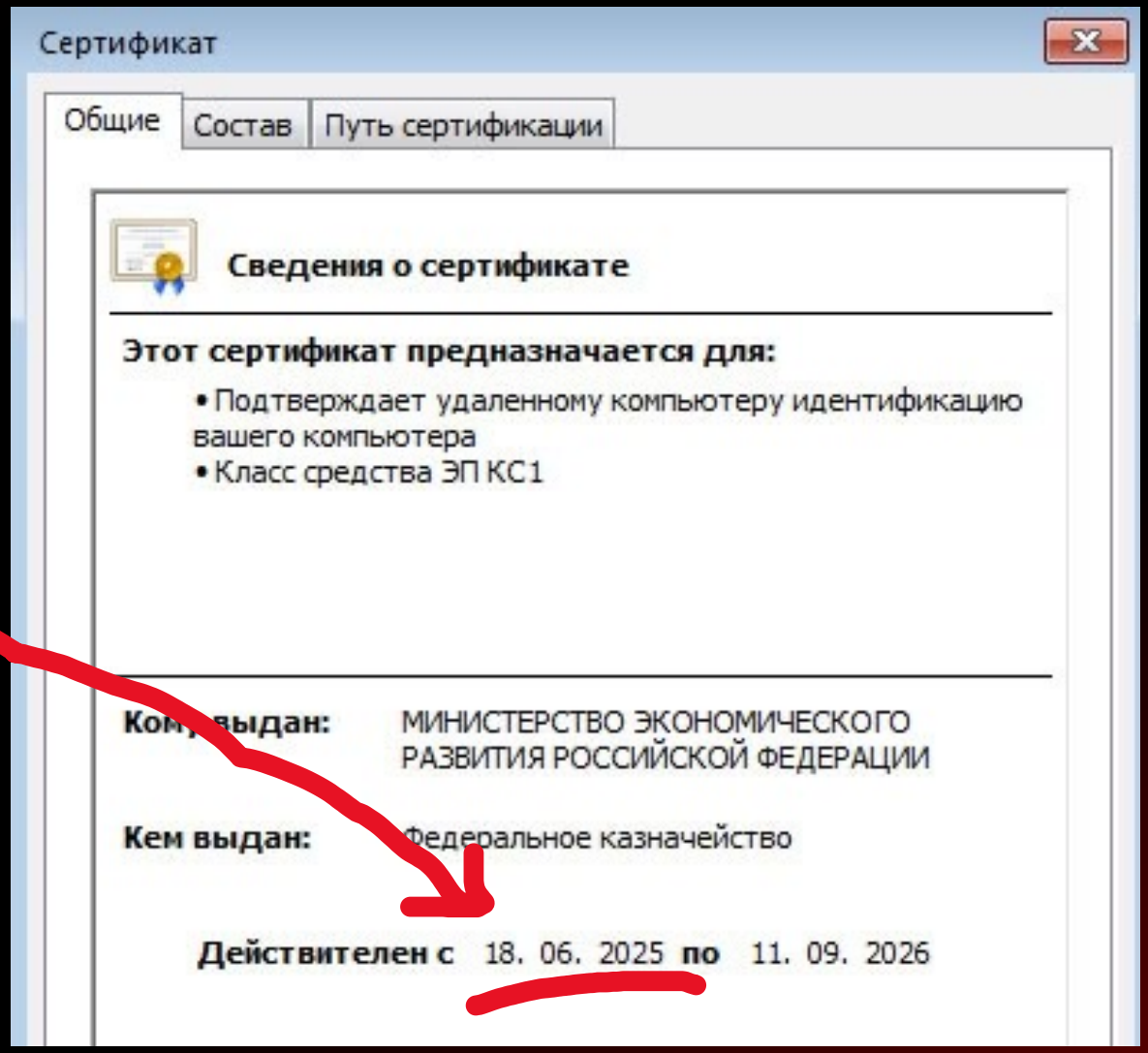
Особенности реализации

- Управление доступом и разграничение прав
  - Регулярная ревизия учётных записей: Например, раз в квартал запрашивать у подрядчика список всех активных учётных записей (логинов) в системах компании и проверять, действительно ли они нужны (особенно после увольнений/ротаций у подрядчика)
  - Технический мониторинг: Настроить логи входа/выхода, включить уведомления о попытках доступа в нерабочее время или не с тех IP-адресов
  - Проверка MFA: Убедиться, что для критичных систем (VPN, админ-доступ) действительно включена многофакторная аутентификация



Кто мониторит сертификаты TLS?





Особенности реализации

- Безопасная обработка и хранение данных
  - Шифрование: Запрашивать у подрядчика, какие протоколы и методы шифрования используются (TLS 1.3/IPSec/IPIir и т. д.), где хранятся ключи. Можно протестировать через внешние сервисы (например, SSL Labs) доступные каналы
  - Проверка резервного копирования: Попросить отчет о бэкапах (периодичность, место хранения), в идеале – план тестирования восстановления (DR-тест)
  - Логирование: Убедиться, что есть логи операций с конфиденциальными данными, и подрядчик может предоставить их вам в случае расследования инцидента





Регистрация событий

- Как подрядчик обеспечивает сбор доказательств несанкционированной деятельности?
- Как долго подрядчик хранит логи? Возможно ли увеличение этого срока?
- Можно ли организовать хранение логов во внешнем хранилище? Как?

https://github.com/BushidoUK/Breach-Report-Collection

Особенности реализации

- Уведомление об инцидентах в заданные сроки
  - Процедуры инцидент-менеджмента: Запрашивать у подрядчика документированные процедуры и как часто они проводили учения или тесты
  - Установленные каналы связи: Проверить, есть ли ответственные контактные лица (24/7?), как быстро подрядчик реагирует на тестовые (или имитационные) инциденты
  - Проверка «реальной» реакции: Если случается мелкий сбой или выявлена уязвимость, смотреть, уведомил ли подрядчик в договорённый срок



Особенности реализации

- Право на аудит и проверки
  - Плановые аудиты: В контракте можно прописать, что раз в год (или в полгода для критичных подрядчиков) вы вправе провести аудит. Составить график, согласовать заранее
  - Внеплановые аудиты: Если обнаружены тревожные сигналы (инцидент, изменения в инфраструктуре подрядчика), можно инициировать внеплановую проверку
  - Документальная проверка: Запрашивать копии протоколов внутренних проверок подрядчика (если у него есть СУИБ, он делает внутренние аудиты)



Особенности реализации

- Управление изменениями (Change Management)
  - Процесс согласования изменений: Требовать уведомлять о любых существенных изменениях (новые технологии, перенастройка сетей, переезд в другой дата-центр) — следить за тем, что такие уведомления действительно поступают
  - Версионность документации: Запрашивать новые версии архитектурных схем, сетевых диаграмм при изменениях
  - Роли и разрешения: Если меняются ключевые сотрудники (тимлиды, админы) у подрядчика, проверять, что их учётные записи корректно переданы или отозваны



Особенности реализации

- Использование субподрядчиков
  - Имена и статусы субподрядчиков: Регулярно уточнять, кого подрядчик привлекает (особенно для критических задач)
  - Flow-down требований: Проверить, действительно ли все пункты «вашего» договора транслируются субподрядчикам (попросить соответствующие контракты или по крайней мере подтверждения)
  - Риски цепочки поставок: Если субподрядчик работает с данными или системами, убедиться, что он также проходит due diligence (опросник, проверка доступа, возможно аудит)



Особенности реализации

- План обеспечения непрерывности (BCP/DR) и реагирования на инциденты
  - Тест BCP/DR: Запрашивать результаты тестов плана непрерывности: когда проводился, какие были итоги, есть ли документированные Lessons Learned
  - Совместный сценарий: Проводить или как минимум планировать совместные учения, если это очень критичный подрядчик (например, «отказ инфраструктуры»)
  - Документы: Проверить, что подрядчик имеет регламент по восстановлению данных (RTO, RPO), согласованный с вашими требованиями



Особенности реализации

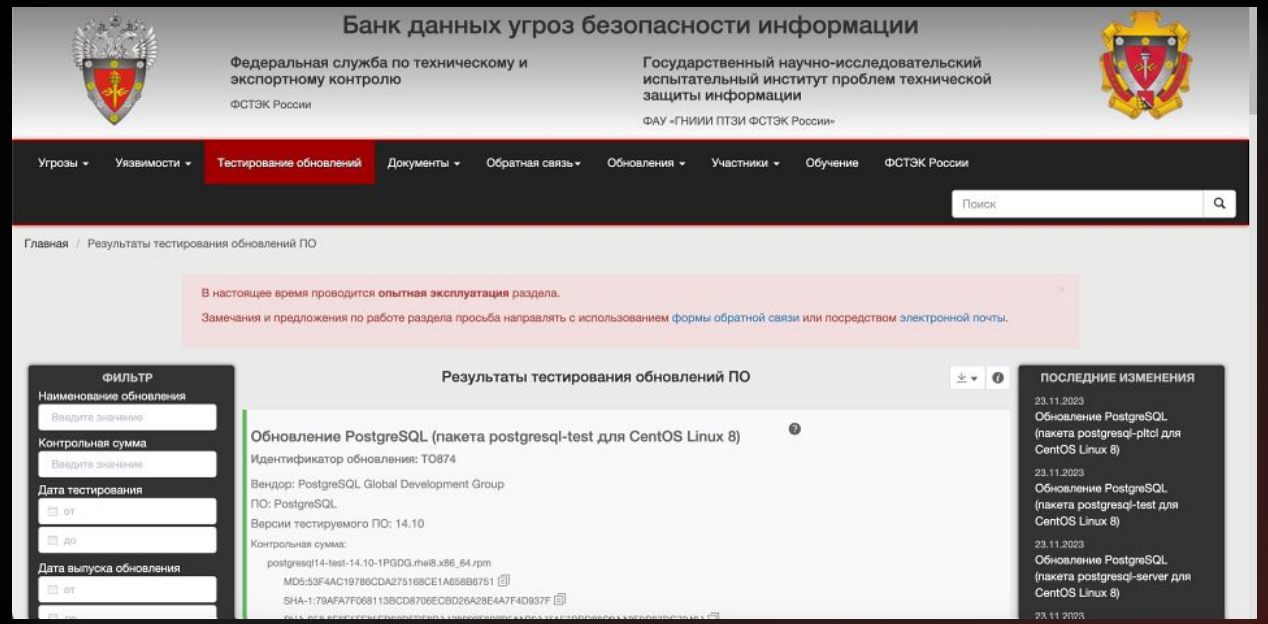
- Условия завершения сотрудничества
  - Акт уничтожения данных: Потребовать у подрядчика «сертификат» или акт, что все данные уничтожены (или переданы) и удалены из резервов
  - Отзыв доступов: Проверять журналы учётных записей, что все логины подрядчика действительно деактивированы, ключи и сертификаты отозваны
  - Проверка фактического удаления: Порой можно сделать тестовый доступ к системам (например, пытаемся зайти от имени бывшего подрядчика) — чтобы убедиться, что его доступ заблокирован





Тестирование обновлений

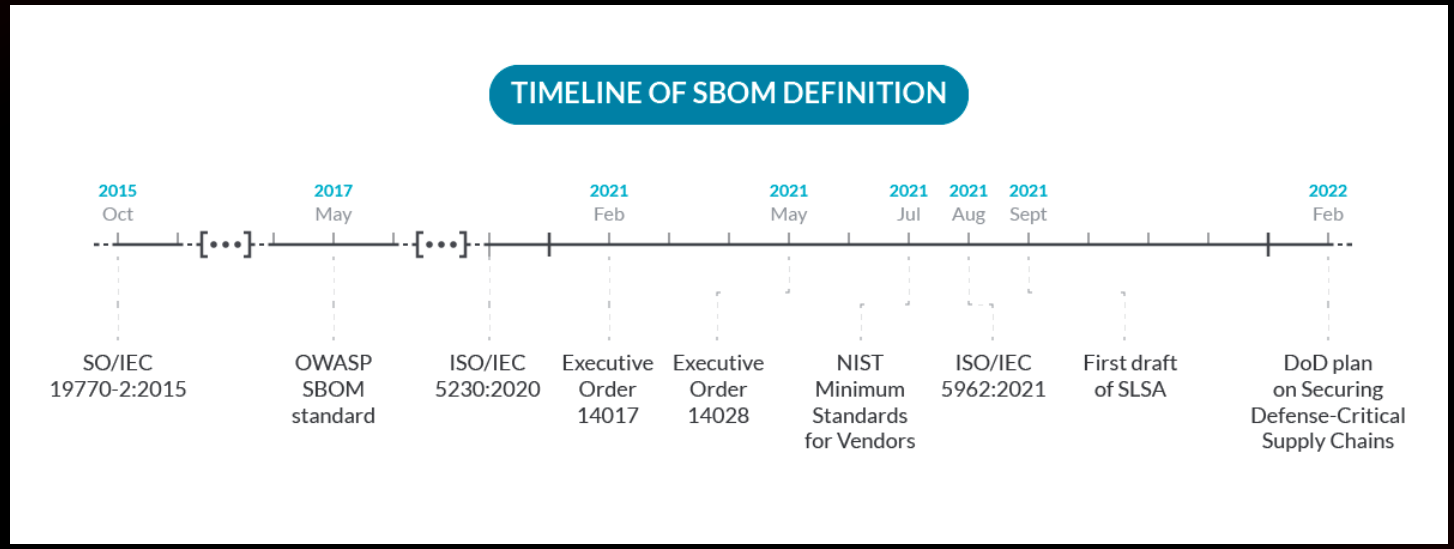
- Песочница
- Тестовый сегмент
- БДУ и методика ФСТЭК



https://bdu.fstec.ru/software-section/updates

Software Bill of Material

- Список всех зависимостей, файлов, лицензий и других компонентов ПО





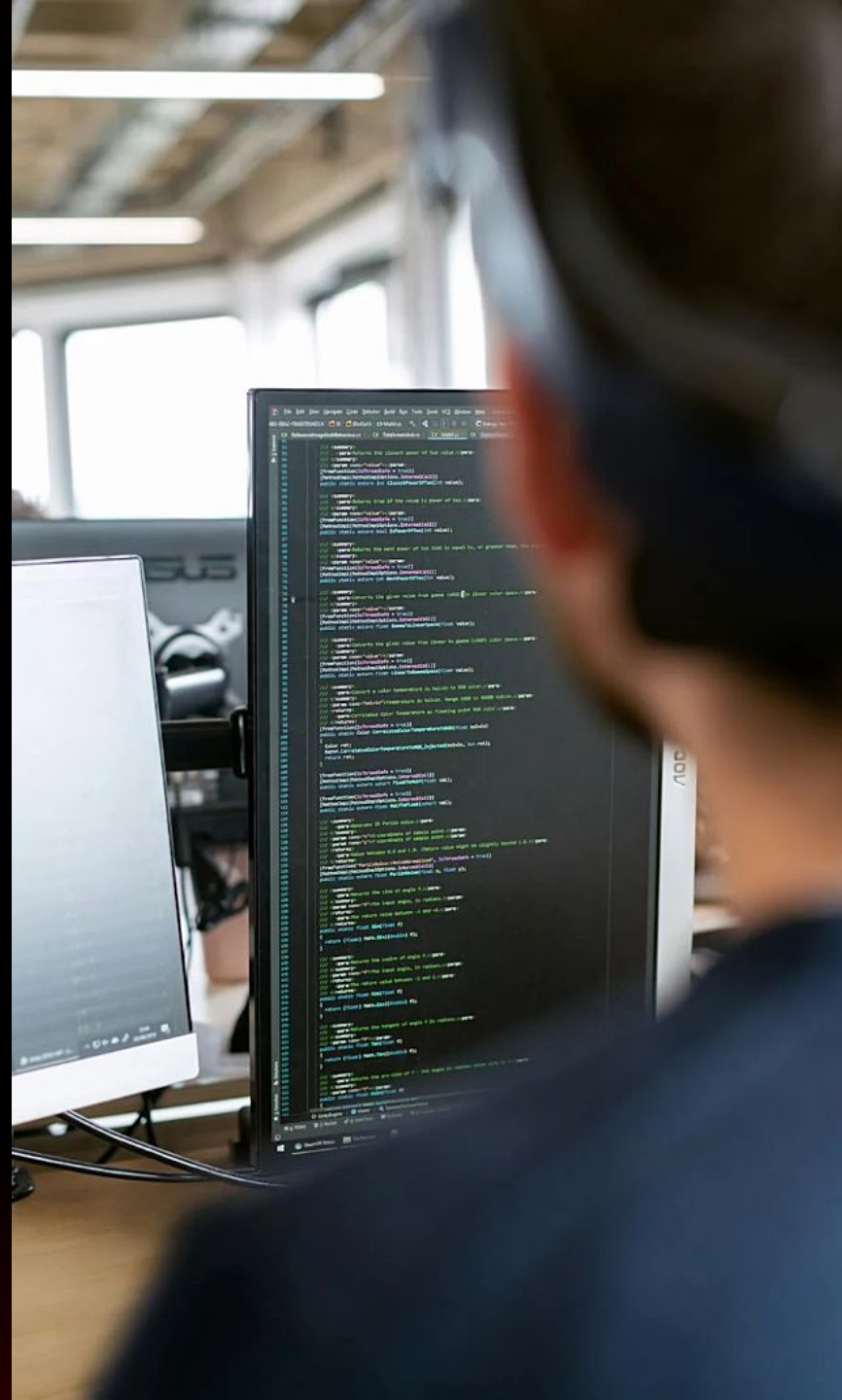
Это все и ФСТЭК требует,
как минимум, для средств защиты!

Генерация SBOM

- Вендор должен предоставлять подписанный SBOM на свое ПО, но мало кто это делает

```
$ syft neo4j:latest
 ✔ Parsed image
 ✔ Cataloged packages      [376 packages]
NAME                              VERSION                    TYPE
CodePointIM                       11.0.15
java-archive
FastInfoset                       1.2.16
java-archive
...
util-linux                        2.36.1-8+deb11u1           deb
wget                              1.21-1+deb11u1             deb
zlib1g                            1:1.2.11.dfsg-2+deb11u1    deb
zstd-jni                          1.5.0-4
java-archive
zstd-proxy                        4.4.8
java-archive
```

Syft



Проверка

- Стартовая проверка (due diligence)
  - Анкеты/опросники:
    - Shared Assessments SIG (Standardized Information Gathering)
    - CSA CAIQ (для облачных сервисов)
    - Собственный чек-лист, составленный на основе ГОСТ/17/21/239/ISO/NIST/SLSA/SSDF
- Аудиторские отчёты и сертификаты: просите у подрядчика SOC 2, ISO 27001, CMMC и т.д.
- Дополнительная валидация: смотреть репутацию подрядчика, отзывы, независимые исследования



Проверка

- Техническая проверка
  - Пентест или сканирование уязвимостей в среде подрядчика (при согласии)
  - Требование вывода на bug bounty или кибериспытания
  - Код-ревью или анализ сборки (для разработчиков ПО)
  - Мониторинг доступов: проверять, какие учетные записи создаются, как часто используются



Проверка

- Регулярный аудит и мониторинг
  - Автоматизация процессов проверки: непрерывное сканирование, регулярные отчёты
  - Обязательные ревизии доступа каждые [X] месяцев
  - Периодический пересмотр опросников и анкет (не раз в 5 лет, а хотя бы ежегодно)



Советы по проверке

- Риско-ориентированный подход: Не надо одинаково глубоко проверять каждого подрядчика. Определите критичных и уделяйте им основное время
- Автоматизация и регулярность: Используйте инструменты для управления учётными записями (IAM, PAM), мониторинга логов, DLP-системы, чтобы не делать всё вручную
- Опросники и чек-листы: Создайте стандартный чек-лист (или анкету) на основе вышеперечисленных требований. Раз в год отправляйте его подрядчику, затем выбирайте из ответов, что требует дополнительной проверки
- Контрактные санкции: Важно прописать, какие последствия будут при несоблюдении требований (штраф, расторжение договора и т. д.) — это заставляет подрядчика воспринимать безопасность всерьёз
- Совместные обучения: Если подрядчик — долгосрочный партнёр, имеет смысл проводить совместные встречи, совместные учения по реагированию на инциденты. Это укрепляет отношения и повышает общий уровень безопасности



Непрерывный цикл

- Контроль изменений: если у подрядчика что-то сильно меняется (слияние, новое ПО, смена локаций), нужно проводить внеплановую проверку (и предусмотреть это в договоре)
- Пересмотр рисков: раз в год (или чаще) обновлять реестр рисков, список недопустимых событий и соответствующие требования
- Процедуры реагирования на инциденты: совместный план действий. Кто, как и когда информирует, какие действия предпринимаются

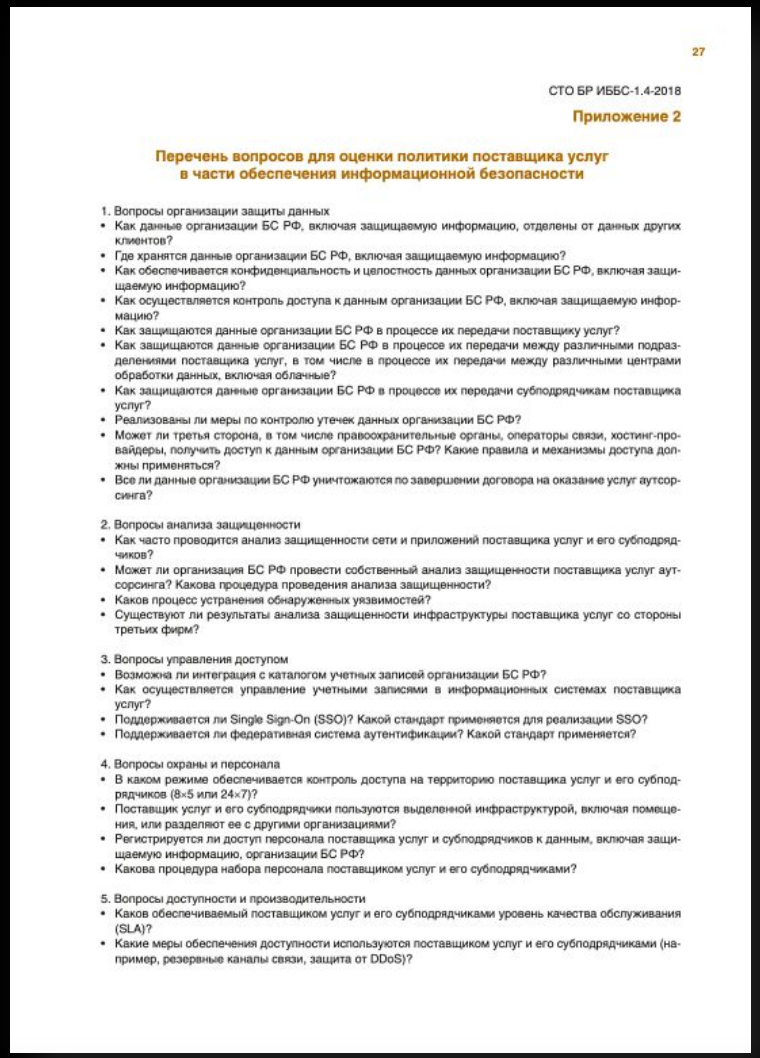


Что говорит закон?

- Банк России
  - СТО БР ИББС-1.4-2018 по безопасности аутсорсинга
  - Управление рисками аутсорсинга на финансовом рынке (доклад)
- ФСТЭК
  - Новый 117-й приказ (с 1.03. 2026)
  - Порядок испытаний и поддержки безопасности средств защиты информации, в состав которых входят заимствованные программные компоненты с открытым исходным кодом от 26 сентября 2024 г. № 240/24/4436
- ФСБ
  - Рекомендации НКЦКИ



Опросник Банка России



Приложение 2

Перечень вопросов для оценки политики поставщика услуг в части обеспечения информационной безопасности

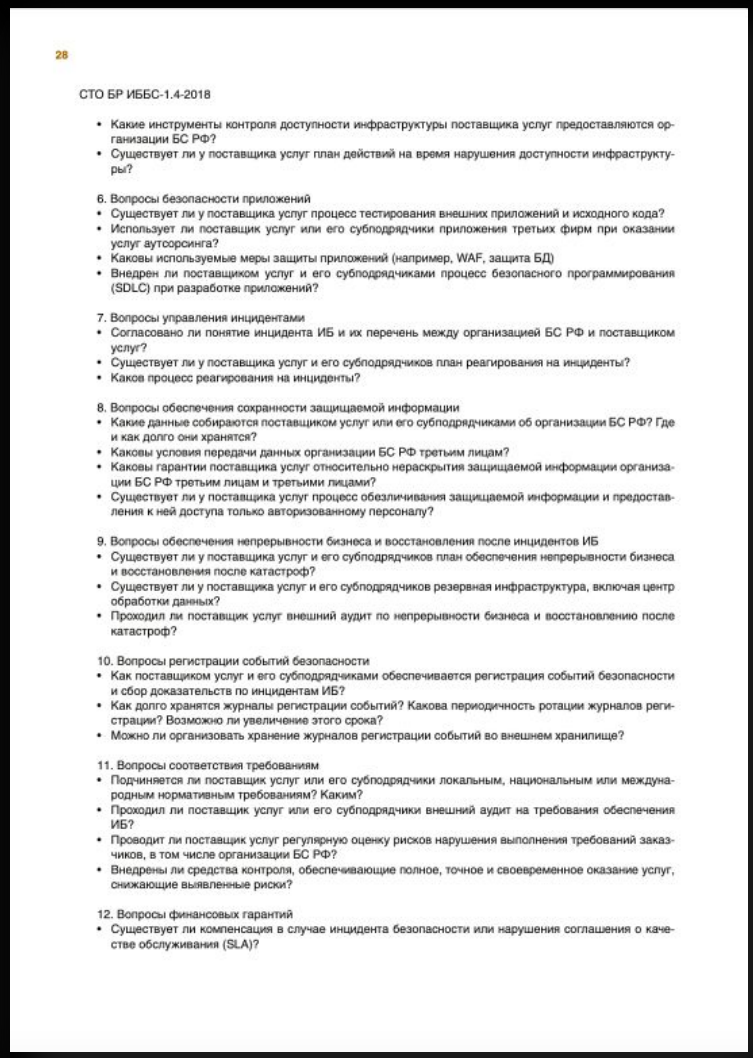
1. Вопросы организации защиты данных
- Как данные организации БС РФ, включая защищаемую информацию, отделены от данных других клиентов?
- Где хранятся данные организации БС РФ, включая защищаемую информацию?
- Как обеспечивается конфиденциальность и целостность данных организации БС РФ, включая защищаемую информацию?
- Как осуществляется контроль доступа к данным организации БС РФ, включая защищаемую информацию?
- Как защищаются данные организации БС РФ в процессе их передачи поставщику услуг?
- Как защищаются данные организации БС РФ в процессе их передачи между различными подразделениями поставщика услуг, в том числе в процессе их передачи между различными центрами обработки данных, включая облачные?
- Как защищаются данные организации БС РФ в процессе их передачи субподрядчикам поставщика услуг?
- Реализованы ли меры по контролю утечек данных организации БС РФ?
- Может ли третья сторона, в том числе правоохранительные органы, операторы связи, хостинг-провайдеры, получить доступ к данным организации БС РФ? Какие правила и механизмы доступа должны применяться?
- Все ли данные организации БС РФ уничтожаются по завершении договора на оказание услуг аутсорсинга?

2. Вопросы анализа защищенности
- Как часто проводится анализ защищенности сети и приложений поставщика услуг и его субподрядчиков?
- Может ли организация БС РФ провести собственный анализ защищенности поставщика услуг аутсорсинга? Какова процедура проведения анализа защищенности?
- Каков процесс устранения обнаруженных уязвимостей?
- Существуют ли результаты анализа защищенности инфраструктуры поставщика услуг со стороны третьих фирм?

3. Вопросы управления доступом
- Возможна ли интеграция с каталогом учетных записей организации БС РФ?
- Как осуществляется управление учетными записями в информационных системах поставщика услуг?
- Поддерживается ли Single Sign-On (SSO)? Какой стандарт применяется для реализации SSO?
- Поддерживается ли федеративная система аутентификации? Какой стандарт применяется?

4. Вопросы охраны и персонала
- В каком режиме обеспечивается контроль доступа на территорию поставщика услуг и его субподрядчиков (8×5 или 24×7)?
- Поставщик услуг и его субподрядчики пользуются выделенной инфраструктурой, включая помещения, или разделяют ее с другими организациями?
- Регистрируется ли доступ персонала поставщика услуг и субподрядчиков к данным, включая защищаемую информацию, организации БС РФ?
- Какова процедура набора персонала поставщиком услуг и его субподрядчиками?

5. Вопросы доступности и производительности
- Каков обеспечиваемый поставщиком услуг и его субподрядчиками уровень качества обслуживания (SLA)?
- Какие меры обеспечения доступности используются поставщиком услуг и его субподрядчиками (например, резервные каналы связи, защита от DDoS)?



- Какие инструменты контроля доступности инфраструктуры поставщика услуг предоставляются организации БС РФ?
- Существует ли у поставщика услуг план действий на время нарушения доступности инфраструктуры?

6. Вопросы безопасности приложений
- Существует ли у поставщика услуг процесс тестирования внешних приложений и исходного кода?
- Использует ли поставщик услуг или его субподрядчики приложения третьих фирм при оказании услуг аутсорсинга?
- Каковы используемые меры защиты приложений (например, WAF, защита БД)
- Внедрен ли поставщиком услуг и его субподрядчиками процесс безопасного программирования (SDLC) при разработке приложений?

7. Вопросы управления инцидентами
- Согласовано ли понятие инцидента ИБ и их перечень между организацией БС РФ и поставщиком услуг?
- Существует ли у поставщика услуг и его субподрядчиков план реагирования на инциденты?
- Каков процесс реагирования на инциденты?

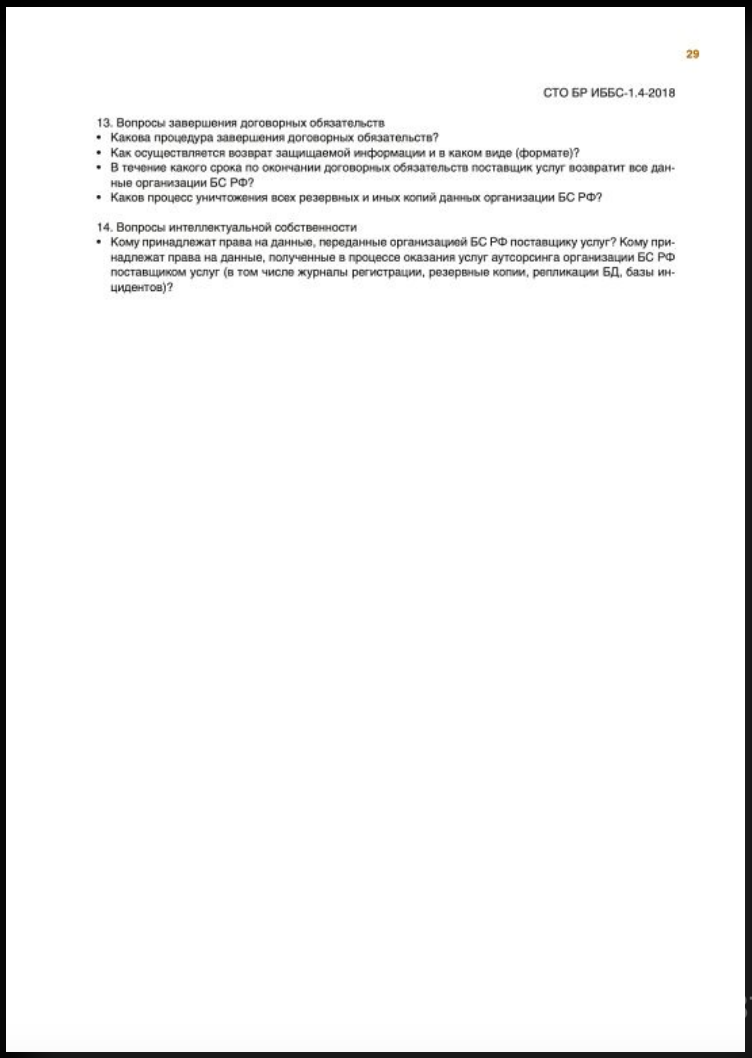
8. Вопросы обеспечения сохранности защищаемой информации
- Какие данные собираются поставщиком услуг или его субподрядчиками об организации БС РФ? Где и как долго они хранятся?
- Каковы условия передачи данных организации БС РФ третьим лицам?
- Каковы гарантии поставщика услуг относительно нераскрытия защищаемой информации организации БС РФ третьим лицам и третьими лицами?
- Существует ли у поставщика услуг процесс обезличивания защищаемой информации и предоставления к ней доступа только авторизованному персоналу?

9. Вопросы обеспечения непрерывности бизнеса и восстановления после инцидентов ИБ
- Существует ли у поставщика услуг и его субподрядчиков план обеспечения непрерывности бизнеса и восстановления после катастроф?
- Существует ли у поставщика услуг и его субподрядчиков резервная инфраструктура, включая центр обработки данных?
- Проходил ли поставщик услуг внешний аудит по непрерывности бизнеса и восстановлению после катастроф?

10. Вопросы регистрации событий безопасности
- Как поставщиком услуг и его субподрядчиками обеспечивается регистрация событий безопасности и сбор доказательств по инцидентам ИБ?
- Как долго хранятся журналы регистрации событий? Какова периодичность ротации журналов регистрации? Возможно ли увеличение этого срока?
- Можно ли организовать хранение журналов регистрации событий во внешнем хранилище?

11. Вопросы соответствия требованиям
- Подчиняется ли поставщик услуг или его субподрядчики локальным, национальным или международным нормативным требованиям? Каким?
- Проходил ли поставщик услуг или его субподрядчики внешний аудит на требования обеспечения ИБ?
- Проводит ли поставщик услуг регулярную оценку рисков нарушения выполнения требований заказчиков, в том числе организации БС РФ?
- Внедрены ли средства контроля, обеспечивающие полное, точное и своевременное оказание услуг, снижающие выявленные риски?

12. Вопросы финансовых гарантий
- Существует ли компенсация в случае инцидента безопасности или нарушения соглашения о качестве обслуживания (SLA)?

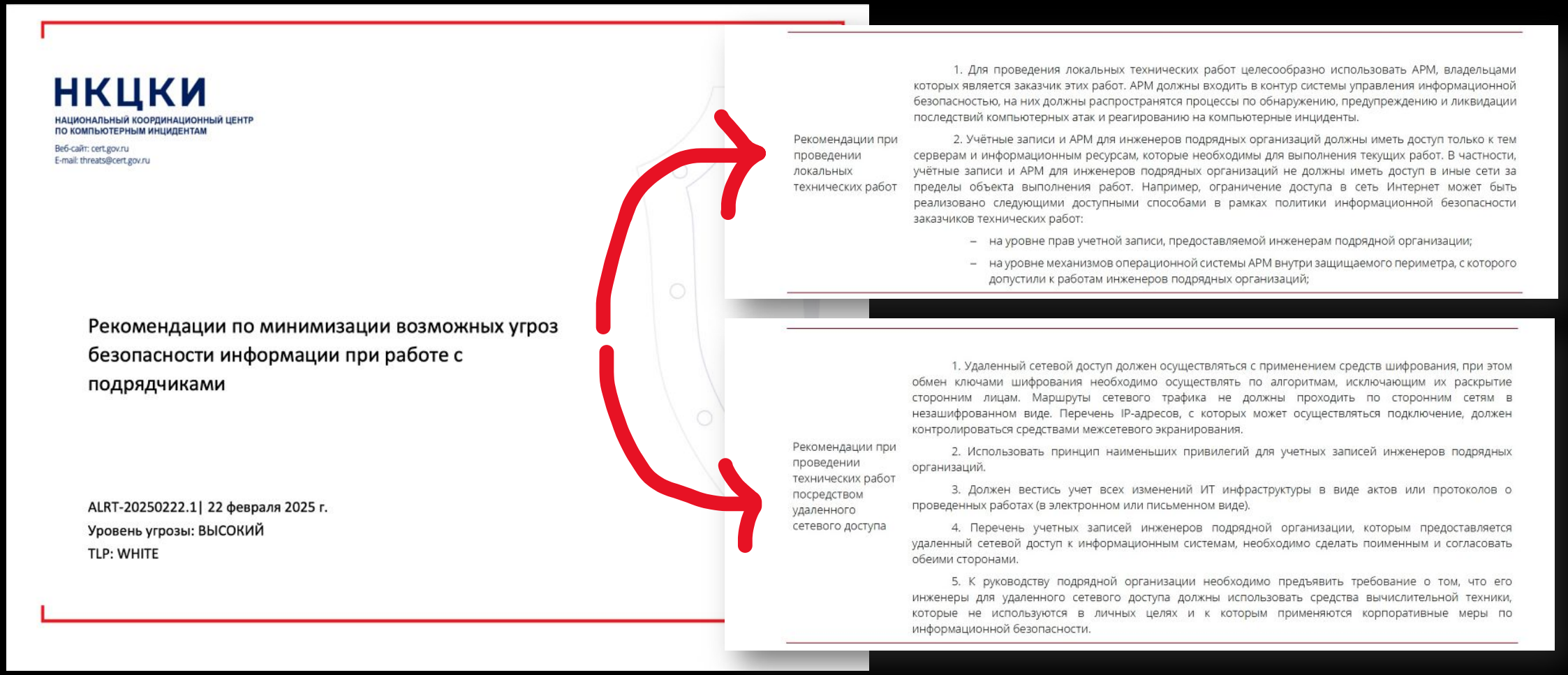


13. Вопросы завершения договорных обязательств
- Какова процедура завершения договорных обязательств?
- Как осуществляется возврат защищаемой информации и в каком виде (формате)?
- В течение какого срока по окончании договорных обязательств поставщик услуг возвратит все данные организации БС РФ?
- Каков процесс уничтожения всех резервных и иных копий данных организации БС РФ?

14. Вопросы интеллектуальной собственности
- Кому принадлежат права на данные, переданные организацией БС РФ поставщику услуг? Кому принадлежат права на данные, полученные в процессе оказания услуг аутсорсинга организации БС РФ поставщиком услуг (в том числе журналы регистрации, резервные копии, репликации БД, базы инцидентов)?

https://www.cbr.ru/Crosscut/LawActs/File/450

Рекомендации НКЦКИ



НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

Рекомендации по минимизации возможных угроз безопасности информации при работе с подрядчиками

ALRT-20250222.1| 22 февраля 2025 г.
Уровень угрозы: ВЫСОКИЙ
TLP: WHITE

Рекомендации при проведении локальных технических работ

1. Для проведения локальных технических работ целесообразно использовать АРМ, владельцами которых является заказчик этих работ. АРМ должны входить в контур системы управления информационной безопасностью, на них должны распространятся процессы по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты.

2. Учётные записи и АРМ для инженеров подрядных организаций должны иметь доступ только к тем серверам и информационным ресурсам, которые необходимы для выполнения текущих работ. В частности, учётные записи и АРМ для инженеров подрядных организаций не должны иметь доступ в иные сети за пределы объекта выполнения работ. Например, ограничение доступа в сеть Интернет может быть реализовано следующими доступными способами в рамках политики информационной безопасности заказчиков технических работ:

- на уровне прав учетной записи, предоставляемой инженерам подрядной организации;
- на уровне механизмов операционной системы АРМ внутри защищаемого периметра, с которого допустили к работам инженеров подрядных организаций;

Рекомендации при проведении технических работ посредством удаленного сетевого доступа

1. Удаленный сетевой доступ должен осуществляться с применением средств шифрования, при этом обмен ключами шифрования необходимо осуществлять по алгоритмам, исключающим их раскрытие сторонним лицам. Маршруты сетевого трафика не должны проходить по сторонним сетям в незашифрованном виде. Перечень IP-адресов, с которых может осуществляться подключение, должен контролироваться средствами межсетевого экранирования.

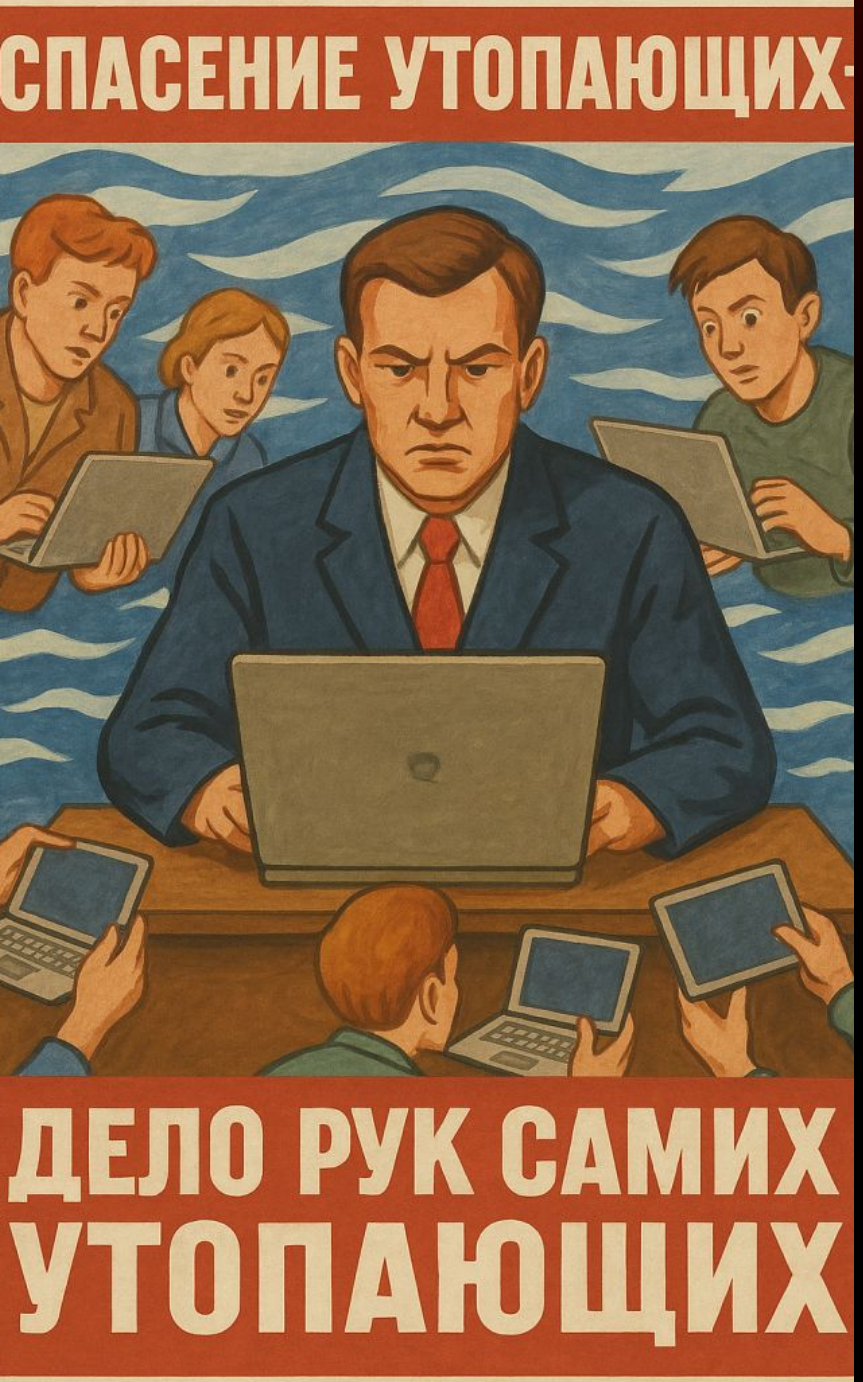
2. Использовать принцип наименьших привилегий для учетных записей инженеров подрядных организаций.

3. Должен вестись учет всех изменений ИТ инфраструктуры в виде актов или протоколов о проведенных работах (в электронном или письменном виде).

4. Перечень учетных записей инженеров подрядной организации, которым предоставляется удаленный сетевой доступ к информационным системам, необходимо сделать поименным и согласовать обеими сторонами.

5. К руководству подрядной организации необходимо предъявить требование о том, что его инженеры для удаленного сетевого доступа должны использовать средства вычислительной техники, которые не используются в личных целях и к которым применяются корпоративные меры по информационной безопасности.

https://gossopka.ru/upload/doc/ALRT-20250222.1.pdf



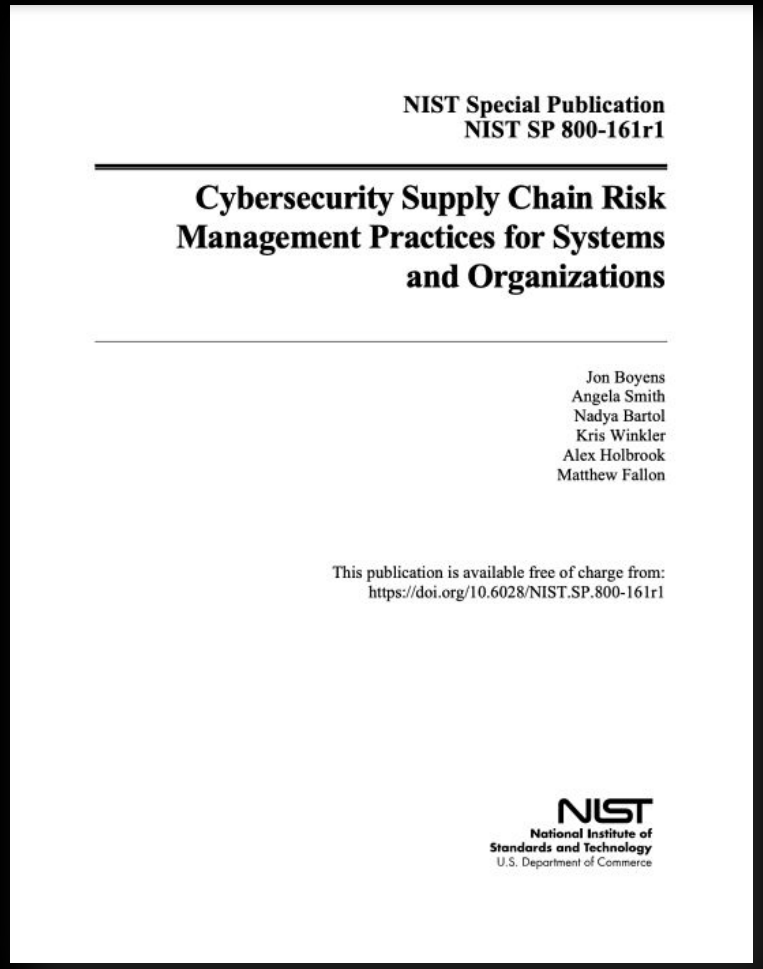
В качестве заключения

- Число атак через подрядчиков растет с каждым годом
- Не стоит игнорировать данное направление, требующее формализации защитных мер и методов оценки их исполнения
- Регуляторы усиливают внимание к этой теме

Спасибо

alukatsky@ptsecurity.com

Что в целом говорит нормативка?



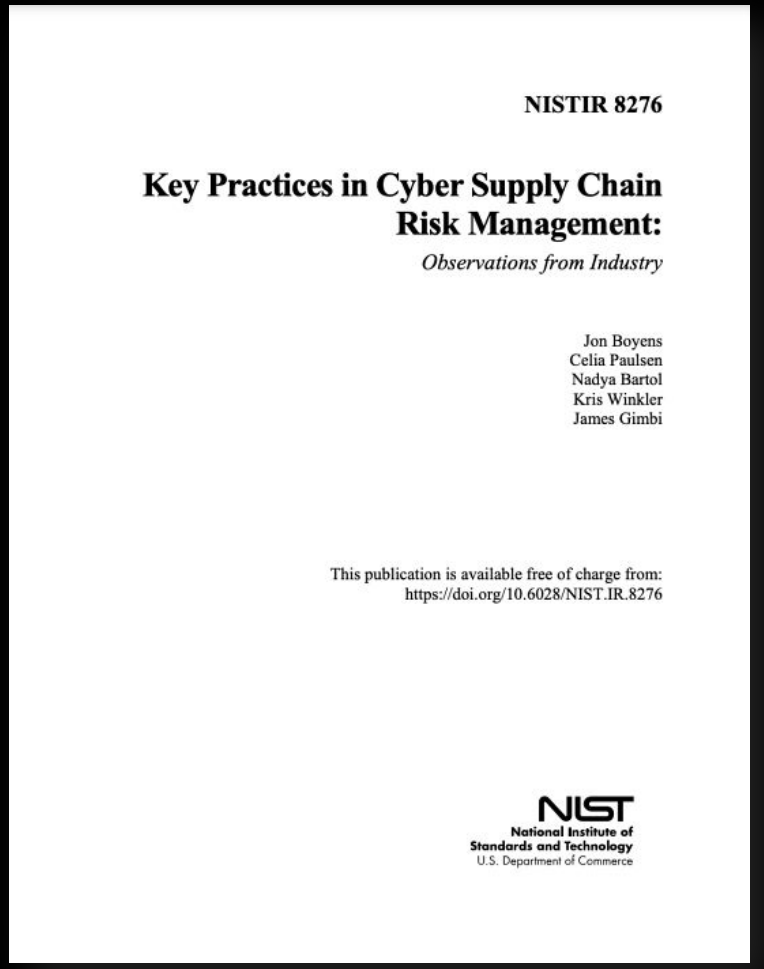
NIST Special Publication
NIST SP 800-161r1

Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

Jon Boyens
Angela Smith
Nadya Bartol
Kris Winkler
Alex Holbrook
Matthew Fallon

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-161r1

NIST
National Institute of Standards and Technology
U.S. Department of Commerce



NISTIR 8276

Key Practices in Cyber Supply Chain Risk Management:

Observations from Industry

Jon Boyens
Celia Paulsen
Nadya Bartol
Kris Winkler
James Gimbi

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8276

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Нормативка

- ISO/IEC 27036 (Information security for supplier relationships)
- ISO/IEC 27036 — это серия стандартов, посвящённая управлению информационной безопасностью в отношениях «заказчик—поставщик».
  - Общие требования
  - Требования по облачным сервисам
  - Управление безопасностью при ИТ-аутсорсинге
  - Рекомендации по внедрению и т.д.
- Фокус: именно как выстраивать и контролировать безопасность на разных этапах сотрудничества с подрядчиками и поставщиками



Нормативка

- NIST SP 800-161 (Supply Chain Risk Management)
  - Полное название: NIST Special Publication 800-161 “Supply Chain Risk Management Practices for Federal Information Systems and Organizations”
  - Разработан Национальным институтом стандартов и технологий США (NIST)
  - Даёт структурированные практики и контрольные меры по оценке и снижению рисков в цепочке поставок (включая выбор, оценку и аудит третьих сторон)
- Фокус: федеральные организации, но методология стала де-факто ориентиром для коммерческого сектора и по всему миру



Нормативка

- TISAX (Trusted Information Security Assessment Exchange) для автопрома
  - Используется европейскими автопроизводителями (VW, Daimler, BMW и др.) для выстраивания единых требований к поставщикам
  - Фокус: оценка информационной безопасности подрядчиков/поставщиков в автомобильном секторе
- CMMC (Cybersecurity Maturity Model Certification)
  - Разработан Министерством обороны США (DoD) для подрядчиков, работающих с оборонным заказом
  - Определяет уровни (maturity levels) кибербезопасности, которые должен продемонстрировать подрядчик, прежде чем получить контракт
  - Фокус: цепочки поставок в военной/оборонной сфере США, но востребован и за её пределами



Нормативка

- FedRAMP (для поставщиков облачных услуг госорганам США)
  - Federal Risk and Authorization Management Program (FedRAMP) — это программа США для авторизации и мониторинга облачных сервисов, предоставляемых федеральным клиентам
  - Фокус: если подрядчик — облачный провайдер, ему необходимо соответствовать FedRAMP, чтобы работать с федеральными органами
- Shared Assessments / SIG
  - Инструмент (в виде анкет и методик оценки), в котором предусмотрены вопросы именно по управлению третьими сторонами и цепочкой поставок
  - Часто используется крупными компаниями и банками для стандартной оценки киберрисков, связанных с подрядчиками
- ENISA (Европейское агентство по кибербезопасности)
  - Выпускает аналитические отчёты и гайды по кибербезопасности, в том числе — по supply chain attacks
  - Пример: ENISA “Threat Landscape for Supply Chain Attacks” и более узкие рекомендации по секторам
  - Фокус: обобщённые европейские рекомендации о том, как выстраивать меры защиты, проводить аудит и анализ рисков именно в цепочках поставок



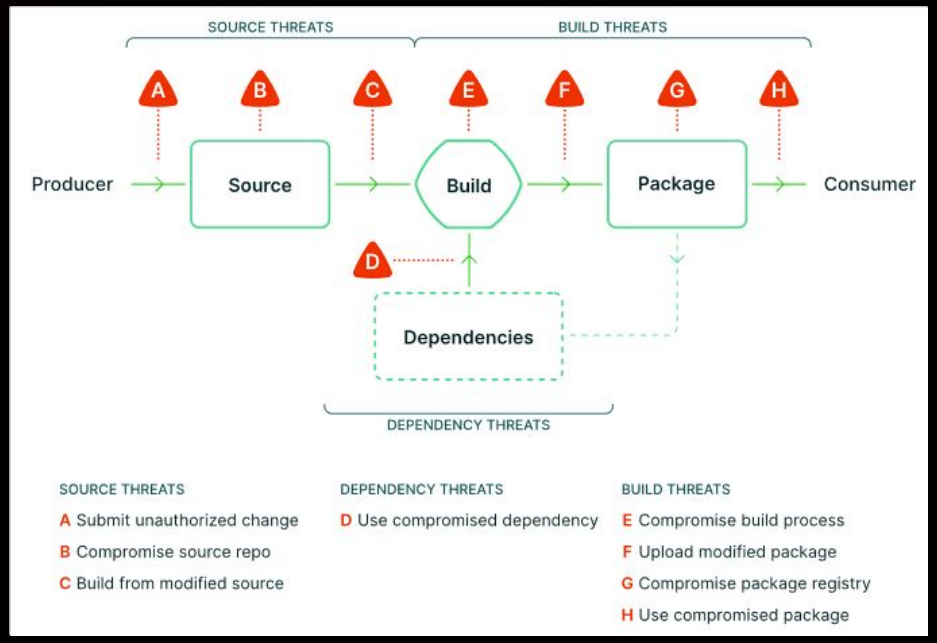
Нормативка

- Australian Cyber Security Centre (ACSC) — выпускает информационные руководства и советы по кибербезопасности, в том числе для управления поставщиками
  - Например, «Security of Network and Infrastructure Supply Chains» и Information Security Manual (ISM)
- NCSC (National Cyber Security Centre) — имеет конкретные гайды по supply chain security
  - «Supply Chain Security Guidance», «12 Principles of Supply Chain Security» и т. д.
- Общие документы
  - Cyber Essentials (UK), ITSG-33 (CA), NIS2 Directive (EU)...



SLSA

- Стандарт Supply-chain Levels for Software Artifacts для защиты ПО от угроз на цепочку поставок





Нормативка для ПО

- SLSA (Supply chain Levels for Software Artifacts)
  - Разработан Google и сообществом OpenSSF (Open Source Security Foundation)
  - Определяет уровни зрелости (Levels 0–4) для процессов сборки, доставки и интеграции ПО. Чем выше уровень, тем более защищён цепной процесс
  - Включает требования к использованию доверенных систем сборки (build systems), проверку целостности артефактов, отслеживание источника (provenance) и т.п.



Нормативка для ПО

- NIST Secure Software Development Framework (SSDF) — SP 800-218
  - Описывает практики безопасной разработки (включая контроль внешних компонентов и библиотек), обязательные проверки кода, валидацию цепочки поставок, риск-менеджмент при использовании open source
  - Имеет связь с рекомендациями из Executive Order 14028 (США), требующего особого внимания к цепочке поставок ПО



Нормативка для ПО

- The Update Framework (TUF) и in-toto
  - TUF — фреймворк для безопасного обновления ПО (исключение атак типа man-in-the-middle и supply chain attacks при распространении пакетов и обновлений)
  - in-toto — расширяет идею TUF и даёт механизмы прослеживаемости (provenance) на всех этапах жизненного цикла ПО — от написания кода до релиза
  - Используются многими крупными проектами, входящими в CNCF (Cloud Native Computing Foundation) и OpenSSF



Нормативка для ПО

- SBOM (Software Bill of Materials)
  - SBOM — это не конкретный стандарт, а концепция (список компонентов, библиотек, лицензий и версий, включённых в конечный продукт)
  - SPDX, CycloneDX — наиболее популярные форматы SBOM
  - Поддерживается рекомендациями и инициативами (например, NTIA — National Telecommunications and Information Administration в США)
  - SBOM способствует прозрачности и позволяет оперативно реагировать на уязвимости в используемых open source-библиотеках



Нормативка для ПО

- OpenSSF (Open Source Security Foundation) инициативы
  - Scorecards — автоматически оценивает репозитории open source-проектов по ряду критериев безопасности (наличие код-ревью, настройки CI/CD, защищённость веток и т.д.)
  - Allstar — GitHub-приложение, которое обеспечивает соответствие репозиториев заданным политикам безопасности
  - CII Best Practices Badge — программа Linux Foundation (часть OpenSSF), позволяющая open source-проектам декларировать соответствие набору требований по качеству и безопасности разработки



Нормативка для ПО

- ISO/IEC 27034 (Application Security)
  - Набор стандартов, посвящённый процессам безопасной разработки и эксплуатации приложений (Application Security Management Process)
  - Включает аспекты оценки риска, внедрения мер защиты на разных этапах SDLC, а также работу с внешними компонентами
- OWASP SAMM (Software Assurance Maturity Model)
  - Фреймворк от OWASP, описывающий уровни зрелости процессов безопасности в разработке
  - Затрагивает управление зависимостями, участие сторонних подрядчиков, анализ архитектуры и т.п.
  - Помогает понять, как «выросла» культура безопасности в команде/организации и какие шаги нужно предпринять для повышения уровня



Нормативка для ПО

- BSIMM (Building Security In Maturity Model)
  - Ещё один популярный модель зрелости безопасной разработки, поддерживаемая компанией Synopsys
  - Основана на реальных практиках более 100 крупных компаний, отслеживает, как они управляют безопасностью кода, библиотек, используемых инструментов
  - Есть разделы, посвящённые работе с open source и внешними поставщиками кода
- OWASP ASVS (Application Security Verification Standard)
  - Стандарт проверки безопасности веб-приложений, в том числе с учётом используемых сторонних компонентов
  - По сути, чеклист, помогающий сформировать требования для различных уровней верификации (проверка зависимостей, обновления, управление ключами и пр.)



Нормативка для ПО

- Proactive Software Supply Chain Risk Management Framework (P-SSCRM)
  - 73 задачи в 4-х группах (управление, продукт, окружение, внедрение)
  - P-SSCRM1 содержит 37 задач из BSIMM13
  - P-SSCRM1 содержит 44 из 183 задач из NIST Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (800-161r1)



Идеи для чеклиста по ПО

- Уровни SLSA: определить, на каком уровне хочет находиться компания (или требует заказчик) — это самая «горячая» тема для ПО, особенно открытого.
- SSDF (SP 800-218): базовый набор практик безопасной разработки, рекомендуемый NIST. Хорошо ложится в чек-лист.
- SBOM-подход: обязательная составляющая для прозрачности цепочки поставок ПО, особенно при массовом использовании open source.
- OWASP SAMM / BSIMM: для общей оценки зрелости процессов безопасной разработки.
- Инструменты: автоматическая проверка зависимостей (Dependency Scanning), анализ кода (SAST/DAST), безопасная конфигурация CI/CD.
- Региональные руководства (NCSC, ENISA, ACSC, CCCS) + Executive Order 14028 (США) для соответствия конкретным требованиям.

