ДЕСЯТИМИНУТКА PRO SMPTE

БЕЗОПАСНОСТЬ МЕДИАПРОИЗВОДСТВА

Олег Березин
член общества инженеров кино и телевидения SMPTE
председатель российской секции SMPTE (suspended since 02/2022)

генеральный директор АО «Невафильм»
член совета директоров Европейского форума цифрового кино
учредитель Высшей школы киноинженеров (Школа инженеров телевидения)
куратор проекта TKT Education

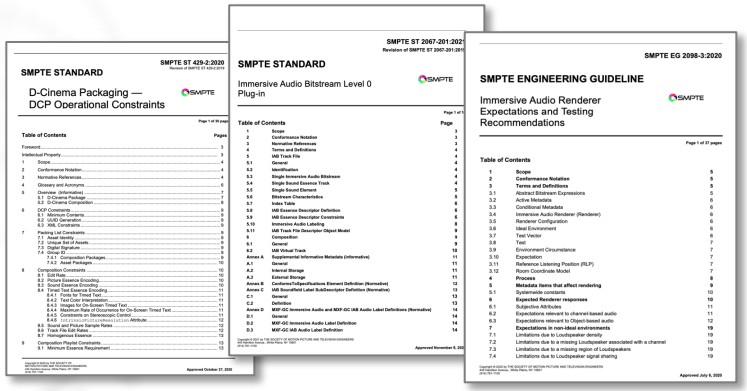
SMPTE – ОБЩЕСТВО ИНЖЕНЕРОВ КИНО И ТЕЛЕВИДЕНИЯ

- Профессиональная ассоциация технических гениев *(так на сайте написано)*, которые делают возможным всем испытывать все преимущества технологий развлечений
- Основано в США в 1916 году как Общество киноинженеров. С 1950 года - SMPTE
- Профессиональная международная организация инженеров кино и телевидения
- Объединяет более **7 000** специалистов из **62** стран мира
- Опубликовано более **820** стандартов, практических рекомендаций и руководств
- 11 комитетов по трем основным направлениям деятельности

- В 1990 году основана советская секция SMPTE (с 1992 года – российская секция)
- Более 50 действующих российских членов *(в т.ч. 30+ студентов)*
- С февраля 2022 г. деятельность российской секции приостановлена

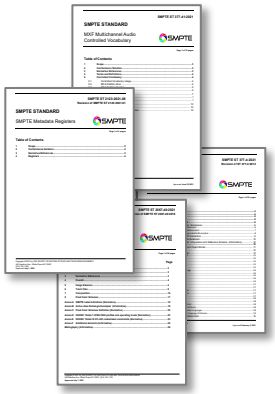
современные вызовы медиаиндустрии

- миграция вещательных технологий в область IT-инфраструктуры
- цифровая кинотеатральная дистрибуция и кинопроекция
- трансформация аппаратных медиапроцессов в программные решения
- иммерсивные технологии: HDR, HFR, HSR (4K/8K), WCG, IMM SOUND, персонализация потребления AV-контента, AR/VR…



Ключевые тренды: IP, UHD/HDR, SaaS (ПО как услуга), Микросервисы, Облака, Виртуализация производства, Конвергенция сред передачи и т.д.

ОСНОВНЫЕ НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТЬ SMPTE



Поддержание творческих контактов между специалистами отрасли. Проведение международных конференций и выставок, помощь национальным секциям в организации локальных мероприятий, веб-трансляции и обсуждения по наиболее актуальным вопросам.

Разработка стандартов. Библиотека нормативных документов SMPTE содержит более 820 стандартов, рекомендованных практик и инженерных руководств по всем разделам кино и телевидения.

SMPTE – основной разработчик международных стандартов ISO в аудиовизуальной сфере.

Обучение и повышение квалификации членов Общества через журнальные публикации, путём проведения семинаров, как в очной форме, так и в сети Интернет, и т.п.

Членство в SMPTE *индивидуальное и платное. Более 100 компаний по всему миру поддерживают работу общества спонсорскими взносами. Среди спонсоров практически все крупнейшие производственные и вещательные компании. Основные расходы – стандарты, образование, конференции, персонал Общества.*

NB! Для студентов символическая оплата членского взноса на период обучения и льготы молодым специалистам

СОВРЕМЕННЫЕ ТРЕНДЫ МЕДИАИНДУСТРИИ

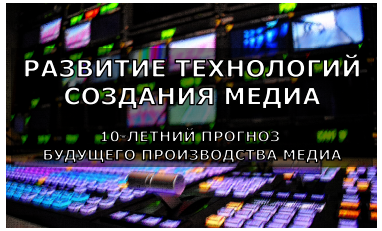
1950-е – начало регулярного телевизионного аналогового вещания, цвет, спутник…
1990-е – цифровизация кино и телепроизводства: Digital Intermediate, Digital Betacam, SDI, аппаратные решения ….
2000-е – цифровая дистрибуция контента: DCP, цифровой кинопоказ, OTT сервисы, DVB
2020-е – IP, облака, микросервисы, системы на базе ПО, XR LED-павильоны, AR/XR, AI/ML…

ОБЛАКО КАК ОСНОВА

1. Все элементы Медиа (сценарии, отснятый материал, звуковые дорожки, VFX и т.д.) будут создаваться либо загружаться сразу непосредственно в облако, без необходимости перемещать их куда-то;
2. Приложения – функционально законченные микропрограммы, станут основой медиапроизводства;
3. Публикация Медиа станет основной функцией воспроизведения и распространения медиаконтента;
4. Архивы как библиотеки с глубоким доступом и технологиями глубокого доступа переместятся в облако, обеспечивающее скорость, наличие и безопасность контента;
5. Сохранение цифровых медиа-данных будет включать возможности будущих трансформаций и монтажа контента.

www.movielabs.com/production-technology

movie labs



БЕЗОПАСНОСТЬ И ДОСТУП

6. Каждый участник проекта идентифицируется и верифицируется, и его права доступа к материалам эффективно и постоянно управляются;
7. Все процессы создания Медиа осуществляются в безопасном окружении, постоянно адаптируемом к изменениям угроз;
8. Индивидуальные элементы Медиа маркируются, отслеживаются и взаимодействуют используя систему универсальных связей и идентификаторов.

ПРОЦЕССЫ КАК ПО

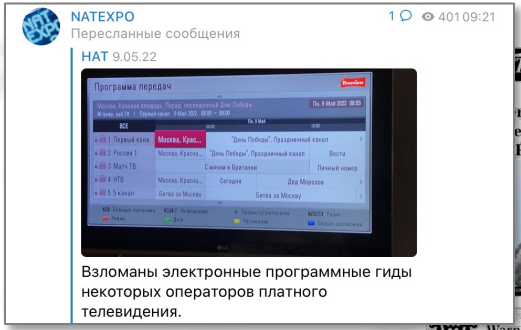
9. Рабочие процессы создания Медиа непрерывны и создаются динамически используя общедоступные интерфейсы, форматы данных и метаданных;
10. Рабочие процессы создаются вокруг итераций и откликов в реальном времени.

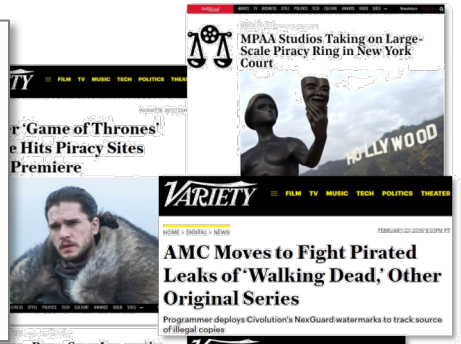
БЕЗОПАСНОСТЬ МЕДИАПРОИЗВОДСТВА. ТИПЫ АТАК

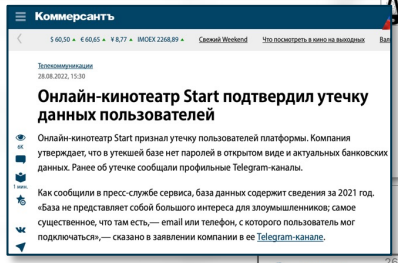
Переход на IP технологии кратно повышает требования к обеспечению безопасности контента и инфраструктуры медиапроизводства

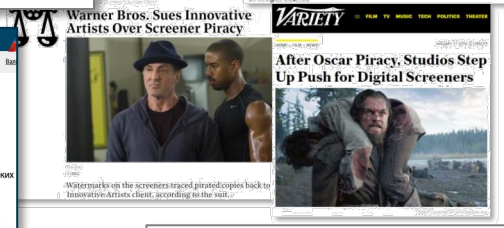
Крупнейшие типы атак на IT-инфраструктуру медиакомпаний:

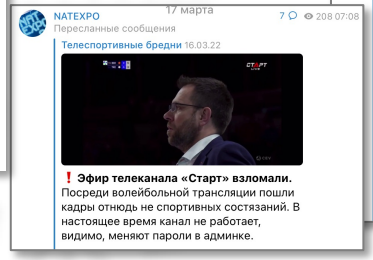
- **кража контента и в т.ч. до начала проката, вещания**
  «Игры престолов»
- **кража данных**
  Sony Pictures – финансовая документация, персональные данные, электронные письма;
  видео-сервис Start – утечка персональных данных 44 млн. пользователей
- **повреждение ПО или файлов, шифрование с целью вымогательства**
  TV5 Monde
- **вставка запрещенной для распространения информации, манипуляции с контентом, подмена контента**
  Россия, Украина, Белоруссия 2020-2023 гг.
- **урон репутации**
  особенно для новых компаний

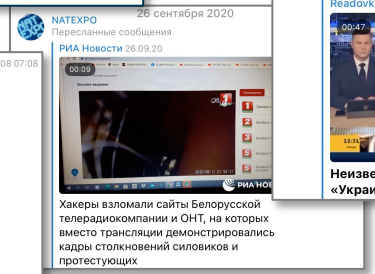












БЕЗОПАСНОСТЬ МЕДИАПРОИЗВОДСТВА. КЛЮЧЕВЫЕ ЗОНЫ БЕЗОПАСНОСТИ

Наибольший урон: утечки на этапе производства

- *как правило, происходят от инсайдеров медиакомпаний*
- *если контент не защищен, утечка может произойти в любое время, из любого места: из production-студий, от владельцев контента, из студий post-production, от поставщиков услуг с третьей стороны, прессы, рейтинговых агентств и учреждений, и т.д.*

Простота копирования контента

- *цифровые копии стали доступнее*

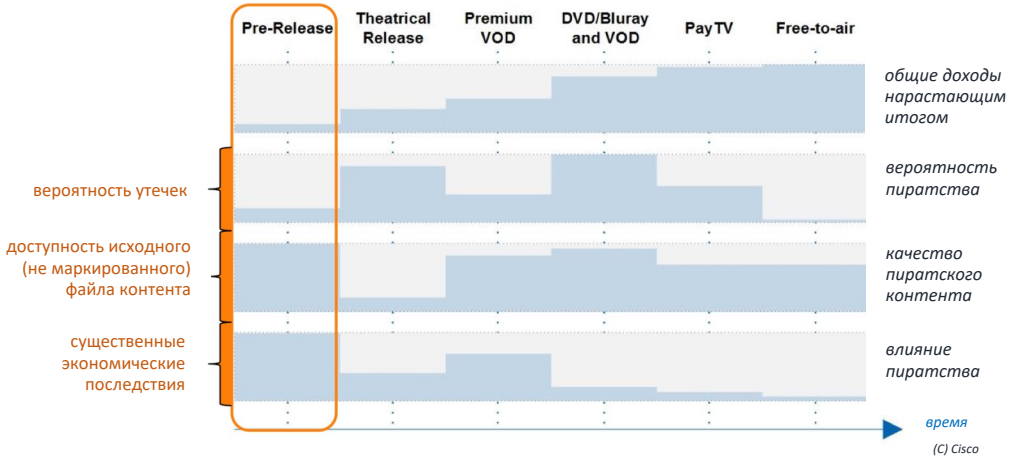
Технологии массового распространения контента

- *доступность неограниченных скоростей соединений*
- *Peer-to-peer технологии*

Высокотехнологичные пиратские сайты

- *продвинутый интерфейс пользователя (UI)*
- *качество не ниже HD*
- *вещание с адаптивным битрейтом на любые устройства*
- *нет ограничений по «окну» релиза*

Любые утечки контента оказывают влияние на доходы медиакомпаний



Ключевые Зоны Безопасности медиапроизводства:

Безопасность контента

- *риск кражи контента либо его компрометации (подмены, манипулирования)*

Безопасность инфраструктуры

- *риск нарушения рабочих процессов, в т.ч. выведение частично либо полностью инфраструктуры медиакомпании из строя;*
- *риск перехвата управления инфраструктурой.*

Человеческий фактор

- *риск злонамеренных действий со стороны персонала медиакомпании (месть, шантаж, подкуп);*
- *нарушение установленных политик безопасности;*
- *недооценка рисков.*

БЕЗОПАСНОСТЬ МЕДИАПРОИЗВОДСТВА. ИНСАЙДЕРЫ

Инсайдеры – категория физических лиц, имеющих доступ к физическим либо цифровым активам организации.

- сотрудники и бывшие сотрудники;
- сотрудники сторонних организаций – контрагенты, фрилансеры, временные работники;
- некоторые категории потребителей.

Инсайдерская угроза – тип риска для организации, исходящий от инсайдеров, имеющих доступ к информации о методах безопасности внутри организации, о данных и о компьютерных системах и сетях.

Типы инсайдерских угроз

- неумышленные действия
- намеренные действия

Меры предупреждения инсайдерских угроз

- осмотрительность и тренинг персонала;
- выявление и предотвращение;
- аппаратный и программный контроль;
- регламенты и процедуры;
- управление правами доступа;
- меры непрерывности бизнеса;
- политики реагирования на инциденты.

Инсайдеры.

80% вредоносных действий совершено в рабочее время на рабочем месте;

81% виновных планировали свои действия заранее;

74% всех типов инцидентов были классифицированы как инсайдерская угроза;

в **81%** случаев мотивом служил финансовый выигрыш.

Чувствительная информация – данные, которые должны быть защищены от неавторизованного доступа для обеспечения приватности или безопасности индивида или организации.

- персональные данные
- коммерческая информация
- классифицированная информация

БЕЗОПАСНОСТЬ МЕДИАПРОИЗВОДСТВА. КЛЮЧЕВЫЕ КОМПОНЕНТЫ

- ✓ Соблюдение формализованных процедур информационной безопасности;
- ✓ Применение технологий шифрования контента;
- ✓ Применение технологий защищенной передачи контента;
- ✓ Реализация архитектуры безопасности IT-инфраструктуры;
- ✓ Обеспечение физической защиты чувствительных устройств и компонентов оборудования;
- ✓ Обеспечение физической защиты контента;
- ✓ Управление контролем доступа пользователей;
- ✓ Применение опознавательных маркеров контента (криминалистических маркеров - fingerprints, watermarks);
- ✓ Обеспечение логирования действий и отчётности персонала и систем;
- ✓ Применение технологий управления правами доступа DRM;
- ✓ Внедрение программ тестирования IT-медиасистем на проникновение, взлом и уязвимости, моделирование атак;
- ✓ Реализация программ аудита и сертификации.

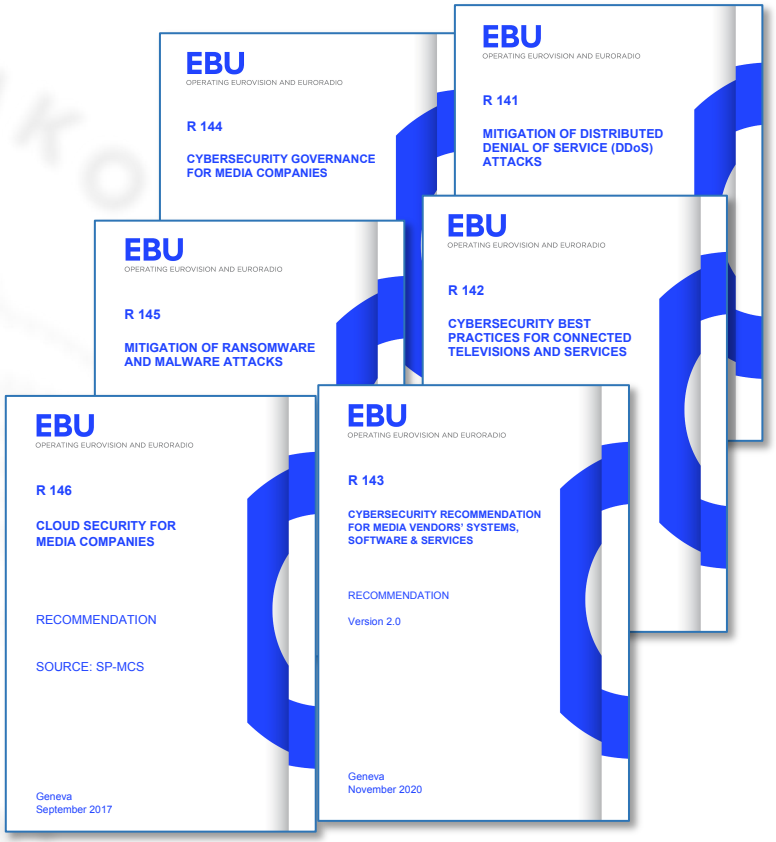
БЕЗОПАСНОСТЬ МЕДИАПРОИЗВОДСТВА. МНОГООБРАЗИЕ СЕРВИСОВ И ТИПОВ КОНТЕНТА

Тип медиапроизводства	типовые услуги и сервисы	типы контента
Производство контента	съемка, монтаж, цветокоррекция, аудиооформление, субтитрирование, надписи, заставки, визуальные эффекты, пакетирование, кодирование	незащищенные исходные материалы самого высокого качества, готовые программы, фильмы, передачи, мастер-файлы контента
курьерские службы и грузоперевозки	сервисы курьеров и доставки, грузоперевозчики	различные виды физических копий контента
рекламные агентства	незавершенный производством контент, трейлеры, ТВ-споты, тизеры, графика, материалы web-рекламы	маркированный контент, частичное/полное содержание, фотографии, клипы и т.д.
службы цифровых медиасервисов	цифровой интермедиэйт, сканирование, реставрация, кодирование, транскодирование, медиа архивы, передача данных и контента и т.д.	частично либо полностью высокого качества контент, части либо полные версии контента
дистрибуция, трансляция, вещание	оформление, кодирование, авторинг, региональные ограничения, версии контента, передача контента, QC	незащищенный немаркированный контент, IMF, MXF
цифровые кинотеатры	производство мастера цифровой копии, тиражирование, управление ключами доступа	немаркированный контент высокого качества, мастер цифровой кинокопии DCDM, цифровая копия DCP
студии визуальных эффектов (VFX)	цифровой пост-продакшен, генерирование изображений, цифровое моделирование и анимация	частично либо полностью высокого качества контент, части либо полные версии контента, кадры, секвенции контента, фотографии, сценарии, раскадровки и т.д.
Приложения и разработка игр	разработка приложений и игр на основе контента	различные виды цифрового контента, сценарии, раскадровки и т.д.
Облачные сервисы	хостинг, дата центры, кодирование, цветокоррекция, шифрование, DRM, передача и доставка, хранение и т.д.	различные виды цифрового контента

БЕЗОПАСНОСТЬ МЕДИАПРОИЗВОДСТВА. РЕКОМЕНДАЦИИ EBU

Опубликованные рекомендации EBU по кибербезопасности

- ✓ R 141. Защита от DDoS Атак;
- ✓ R 142. Общие практики по кибербезопасности для стриминговых сервисов (Connected TV & Services);
- ✓ R 143. Рекомендации по кибербезопасности для для поставщиков систем, программного обеспечения и сервисов в медиасфере;
- ✓ R 144. Управление кибербезопасностью для медиакомпаний;
- ✓ R 145. Защита от атак программ-вымогателей и вредоносного ПО;
- ✓ R 146. Безопасность в облачных сервисах для медиакомпаний;
- ✓ R148. Кибербезопасность для вендров медиасистем, ПО и услуг.



БЕЗОПАСНОСТЬ МЕДИАПРОИЗВОДСТВА. РЕКОМЕНДАЦИИ WBC

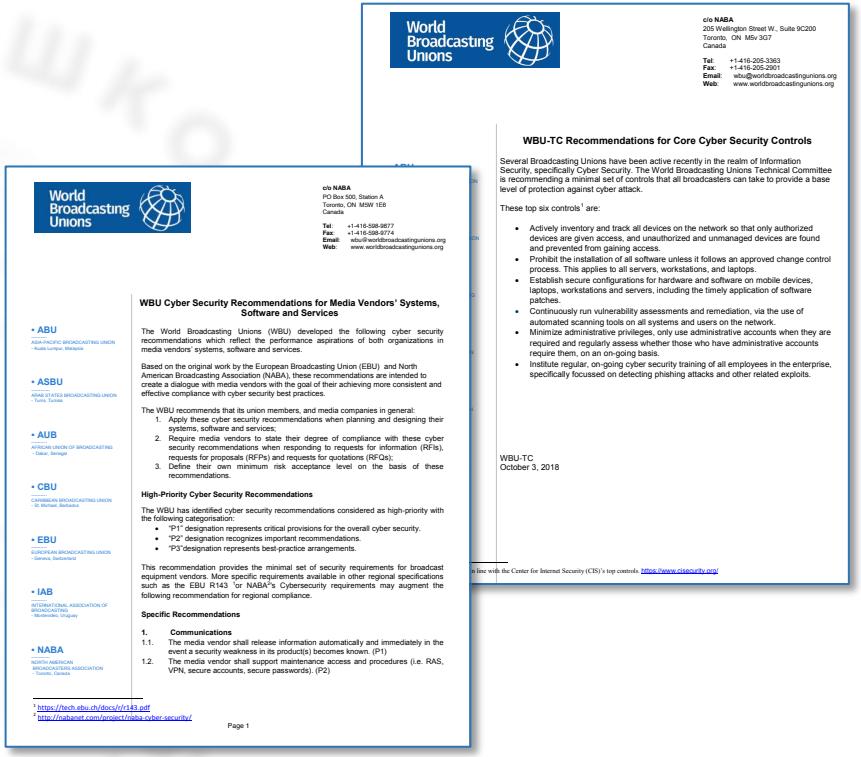
«Рекомендации **WBU-TC** по кибербезопасности для поставщиков систем, ПО и сервисов в медиасфере»

«Рекомендации **WBU-TC** по управлению ключевыми компонентами кибербезопасности»

- Комбинация требований EBU, NABA, ABU и других сообществ телевещателей;
- Рекомендации (не требования) в области: коммуникации, аутентификация, управление, документирование, шифрование, конфигурация сетей;
- Рекомендованы к включению в индустриальные документы для обеспечения потенциальными поставщиками должного уровня кибербезопасности;
- Приоритизация рекомендаций

Готовятся к публикации:

- *Базовая «кибергигиена» для медиакомпаний*
- *Кибербезопасность при использовании облачных медиасервисов*



World Broadcasting Unions

c/o NABA
PO Box 500, Station A
Toronto, ON M5W 1E6
Canada

Tel: +1-416-598-9877
Fax: +1-416-598-9774
Email: wbu@worldbroadcastingunions.org
Web: www.worldbroadcastingunions.org

WBU Cyber Security Recommendations for Media Vendors' Systems, Software and Services

The World Broadcasting Unions (WBU) developed the following cyber security recommendations which reflect the performance aspirations of both organizations in media vendors' systems, software and services.

Based on the original work by the European Broadcasting Union (EBU) and North American Broadcasting Association (NABA), these recommendations are intended to create a dialogue with media vendors with the goal of their achieving more consistent and effective compliance with cyber security best practices.

The WBU recommends that its union members, and media companies in general:

1. Apply these cyber security recommendations when planning and designing their systems, software and services;
2. Require media vendors to state their degree of compliance with these cyber security recommendations when responding to requests for information (RFIs), requests for proposals (RFPs) and requests for quotations (RFQs);
3. Define their own minimum risk acceptance level on the basis of these recommendations.

High-Priority Cyber Security Recommendations

The WBU has identified cyber security recommendations considered as high-priority with the following categorisation:

- "P1" designation represents critical provisions for the overall cyber security.
- "P2" designation recognizes important recommendations.
- "P3"designation represents best-practice arrangements.

This recommendation provides the minimal set of security requirements for broadcast equipment vendors. More specific requirements available in other regional specifications such as the EBU R143 "or NABA"s Cybersecurity requirements may augment the following recommendation for regional compliance.

Specific Recommendations

1. Communications

1.1. The media vendor shall release information automatically and immediately in the event a security weakness in its product(s) becomes known. (P1)

1.2. The media vendor shall support maintenance access and procedures (i.e. RAS, VPN, secure accounts, secure passwords). (P2)

[1] https://tech.ebu.ch/docs/r/r143.pdf
[2] http://nabanet.com/project/naba-cyber-security/

Page 1

• ABU — ASIA-PACIFIC BROADCASTING UNION — Kuala Lumpur, Malaysia
• ASBU — ARAB STATES BROADCASTING UNION — Tunis, Tunisia
• AUB — AFRICAN UNION OF BROADCASTING — Dakar, Senegal
• CBU — CARIBBEAN BROADCASTING UNION — St. Michael, Barbados
• EBU — EUROPEAN BROADCASTING UNION — Geneva, Switzerland
• IAB — INTERNATIONAL ASSOCIATION OF BROADCASTING — Montevideo, Uruguay
• NABA — NORTH AMERICAN BROADCASTERS ASSOCIATION — Toronto, Canada

World Broadcasting Unions

c/o NABA
205 Wellington Street W., Suite 9C200
Toronto, ON M5v 3G7
Canada

Tel: +1-416-205-3363
Fax: +1-416-205-2901
Email: wbu@worldbroadcastingunions.org
Web: www.worldbroadcastingunions.org

WBU-TC Recommendations for Core Cyber Security Controls

Several Broadcasting Unions have been active recently in the realm of Information Security, specifically Cyber Security. The World Broadcasting Unions Technical Committee is recommending a minimal set of controls that all broadcasters can take to provide a base level of protection against cyber attack.

These top six controls[1] are:

- Actively inventory and track all devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.
- Prohibit the installation of all software unless it follows an approved change control process. This applies to all servers, workstations, and laptops.
- Establish secure configurations for hardware and software on mobile devices, laptops, workstations and servers, including the timely application of software patches.
- Continuously run vulnerability assessments and remediation, via the use of automated scanning tools on all systems and users on the network.
- Minimize administrative privileges, only use administrative accounts when they are required and regularly assess whether those who have administrative accounts require them, on an on-going basis.
- Institute regular, on-going cyber security training of all employees in the enterprise, specifically focussed on detecting phishing attacks and other related exploits.

WBU-TC
October 3, 2018

[1] In line with the Center for Internet Security (CIS)'s top controls. https://www.cisecurity.org/

БЕЗОПАСНОСТЬ МЕДИАПРОИЗВОДСТВА. СЕРТИФИКАЦИЯ И НОРМАТИВНЫЕ ДОКУМЕНТЫ

MPA

CDSA Content Delivery & Security Association

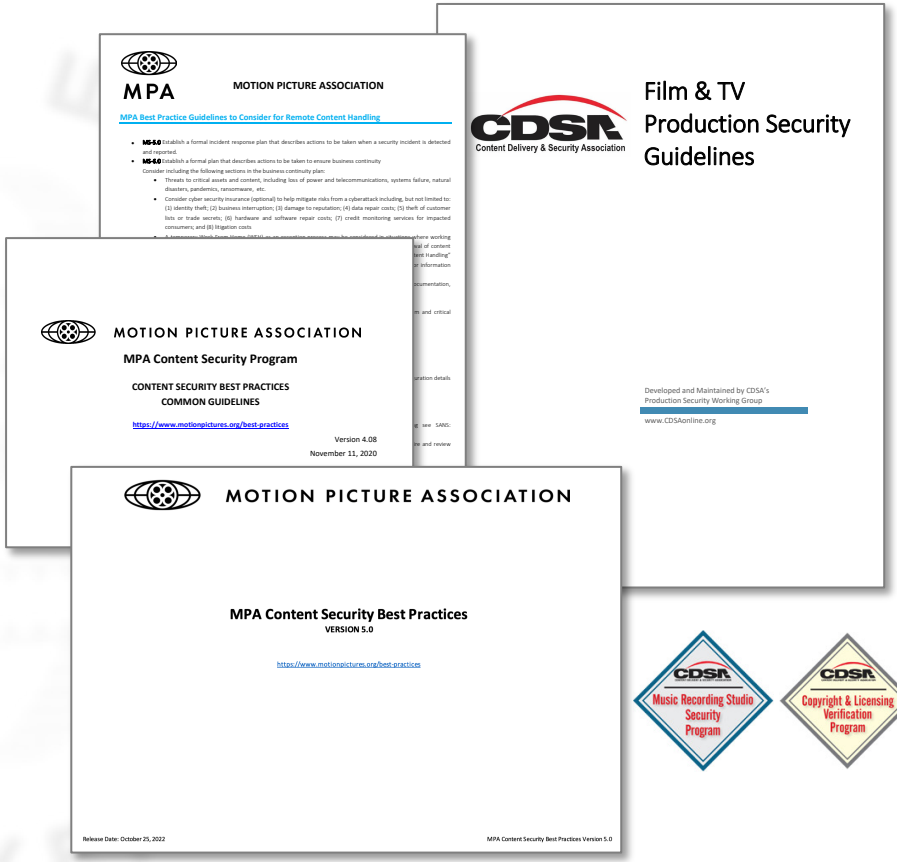
TPN TRUSTED PARTNER NETWORK

EBU

NABA

World Broadcasting Unions

Технический комитет по стандартизации
«Криптографическая защита информации» (ТК 26)



CDSA Music Recording Studio Security Program

CDSA Copyright & Licensing Verification Program

БЕЗОПАСНОСТЬ МЕДИАПРОИЗВОДСТВА. ПРОГРАММЫ СЕРТИФИКАЦИИ MPA TPN

СИСТЕМА МЕНЕДЖМЕНТА

организация и управление

- система контроля процедур безопасности
- управление рисками
- организация безопасности
- политики и процедуры
- реагирование на инциденты
- процедуры непрерывности бизнеса
- управление изменениями производственных процессов
- описание рабочих процессов
- разделение ролей
- фоновый мониторинг
- соглашение о конфиденциальности
- мониторинг действий третьих сторон

ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ

производственная среда

- входы/выходы
- посетители (вход/выход)
- идентификация посетителей
- безопасность периметра
- сигнализация
- авторизация
- электронный контроль доступа
- ключи, мастер-ключи
- видеонаблюдение
- логирование и мониторинг доступа
- процедуры досмотра

управление активами

- контроль перемещений физических носителей и оборудования
- контроль складских запасов (медиатеки)
- контроль чистых носителей контента
- контроль материалов клиента
- уничтожение/разрушение контента

управление доставкой

- отправка материалов (курьеры и т.д.)
- приемка материалов (курьеры и т.д.)
- маркировка (в т.ч. секретные названия)
- упаковка материалов
- транспортировка
- условия хранения (температура, влажность и т.д.)

ЦИФРОВАЯ БЕЗОПАСНОСТЬ

производственная инфраструктура

- файервол/WAN/ безопасность периметра
- интернет
- LAN
- Wi-Fi/WLAN
- безопасность устройств Tx/Rx
- безопасность системы (в целом)
- управление аккаунтами пользователей
- аутентификация
- логирование и мониторинг

управление контентом

- безопасность мобильных устройств

передача контента

- технологии защиты контента (водяные знаки, шифрование)
- контроль перемещений контента
- системы передачи и обмена данными
- методология передачи данных между устройствами
- клиентские порталы

Motion Picture Association of America

TPN TRUSTED PARTNER NETWORK

***Цель**: усиления процесса защиты контента на протяжении всего жизненного цикла: производство, post-production, маркетинг и дистрибуция.*
***Достигается** распространением лучших практик по обеспечению безопасности контента и оценки соответствия стандартам безопасности в медиасфере для производящих и дистрибуционных компаний.*

БЕЗОПАСНОСТЬ МЕДИАПРОИЗВОДСТВА. ПОЧЕМУ ЭТО ВАЖНО?

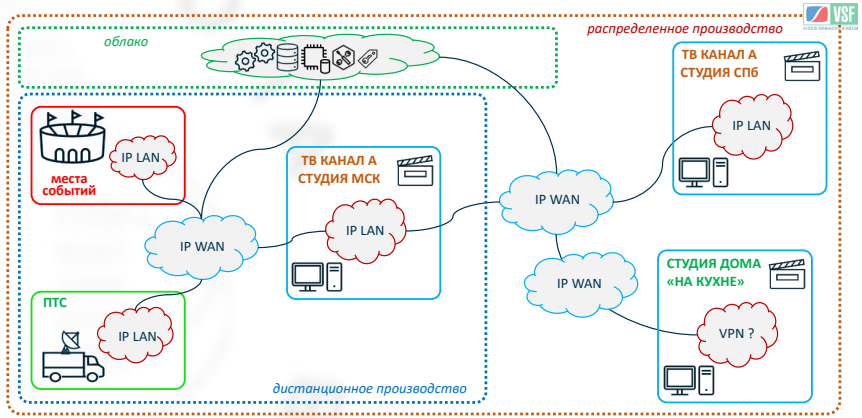
Медиаиндустрия с одной стороны, и IT-мир только начинают движение навстречу друг к другу.

Разрыв между индустриальными сообществами кино и ТВ и IT-сообществами создаёт угрозу безопасности медиапроизводства.

Вопросы IT-инфраструктуры сегодня не охватываются индустриальными стандартизирующими сообществами в медиаиндустрии – SMPTE, EBU, AES, VSF и и др.

Вопросами стандартизации в IT-сфере занимаются другие сообщества – IETF, IEEE, W3C и другие

Ключевая проблема
компетенции и мышление инженеров медиаиндустрии в IT-сфере



Вне зависимости от эффективности технологий виртуального, распределённого, дистанционного производства, облачных сервисов, ИИ, IoT, ST 2110, вычислительных технологий, дата-центров, съемки в XR LED-павильонах; либо цифрового оборудования и технологических процессов в любой сфере медиа: кинопроизводства, телевидения, вещания или прямых трансляций событий – ***контент остаётся общим знаменателем и весь контент перемещается в физическом мире!***

БЕЗОПАСНОСТЬ МЕДИАПРОИЗВОДСТВА. CASE#1: ДОВЕРЕННЫЕ ГРАНИЦЫ МЕЖДУ МЕДИАКОМПЛЕКСАМИ

SMPTE PCD RP 2129:20xx
SMPTE Public Committee Draft
Inter Entity Trust Boundary

Доверенные границы медиакомплексов

- между подразделениями одной медиакомпании
- между разными медиакомпаниями
- между медиакомпаниями и ISP

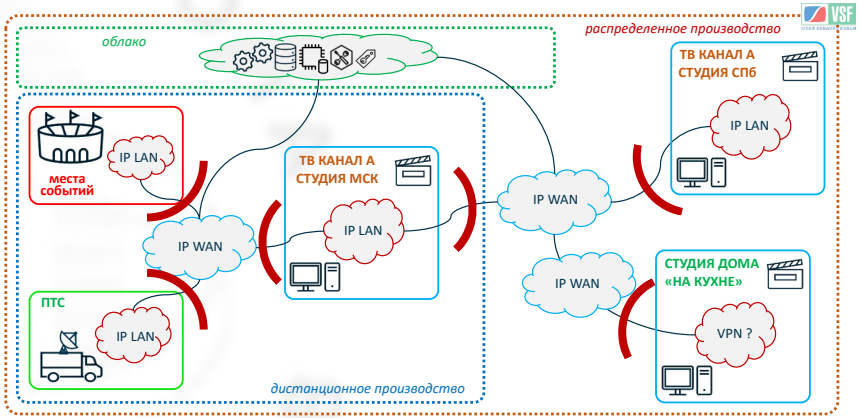
как правило, речь о географически разнесенных компаниях

Доверенная граница – функционал, разворачиваемый в точке демаркации между двумя медиакомплексами либо географически разнесенных подразделениями одного медиакомплекса, который мониторит, управляет и контролирует весь линейный медиатрафик, отфильтровывая ненужный трафик.

Традиционно, трафик между медиакомплексами сегодня – это IP-потоки (multicast или unicast) линейных медиапотоков, стандартизированных SMPTE

«композитные медиапотоки» – ST 2022

«компонентные медиапотоки» – ST 2110

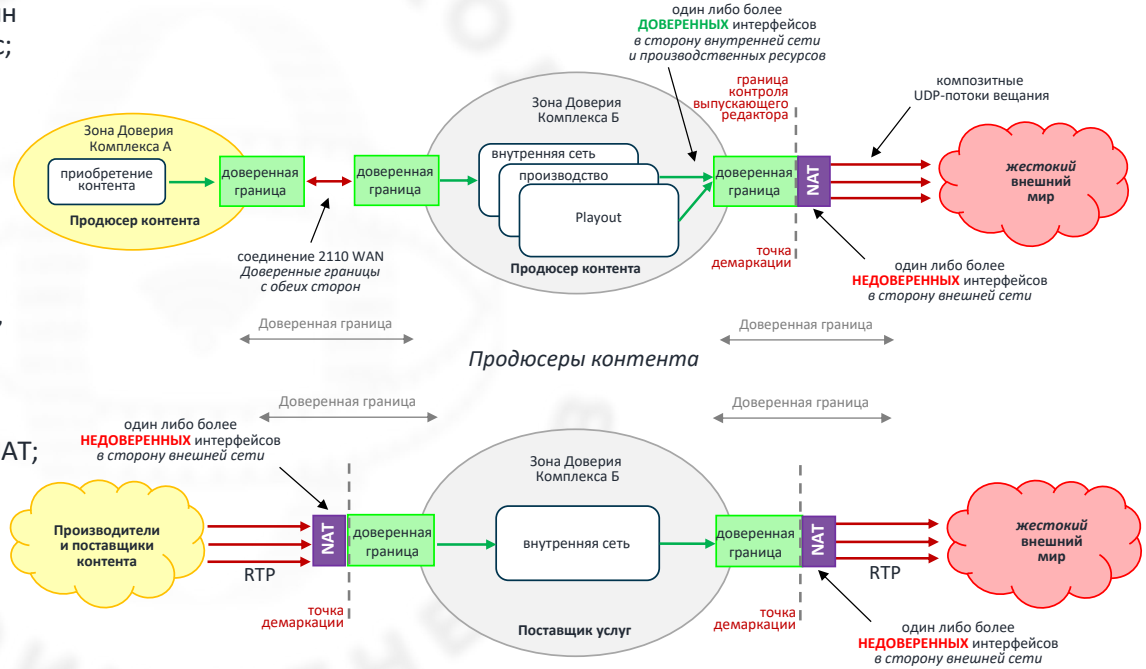


БЕЗОПАСНОСТЬ МЕДИАПРОИЗВОДСТВА. CASE#1: ДОВЕРЕННЫЕ ГРАНИЦЫ МЕЖДУ МЕДИАКОМПЛЕКСАМИ

SMPTE PCD RP 2129:20xx
SMPTE Public Committee Draft
Inter Entity Trust Boundary SMPTE

Доверенные интерфейсы соединяют собственные (внутренние) сети и адресное пространство медиакомплекса
Недоверенные интерфейсы соединяют сети разных медиакомплексов через неконтролируемые публичные WAN сети

- каждый медиакомплекс должен иметь как минимум один доверенный интерфейс и один недоверенный интерфейс;
- Должен убивать все пакеты, полученные через недоверенный интерфейс, за исключением пакетов, разрешенных одним либо несколькими правилами файрвола; и выпускать разрешенные пакеты через внутренние доверенные интерфейсы;
- Для недоверенных и доверенных интерфейсов должны быть разные правила файрвола;
- должен фильтровать все пакеты на основании источника, назначения unicast, адресов multicast, портов UDP, тэгов VLAN по правилам 2,3,4 Уровней OSI;
- должен оперировать только UDP-пакетами;
- должен обрабатывать отдельно каждый пакет на этапе NAT;
- Должен обрабатывать RTP-заголовки где необходимо
- Оба типа интерфейсов должны соединяться с сетевым оборудованием стандартными интерфейсами со стандартной пропускной способностью:
  1 Гб/с – SFR, 10 Гб/с – SFR+, 25 Гб/с – SFR28;
- поддерживать стандартную полезную нагрузку ST2022, ST2110 и будущих стандартов + ST2022-7, + FEC, +ARQ, + … ;
- может фильтровать трафик по PT RTP-пакетов и т.д.



Сквозное линейное вещание через Поставщика услуг

БЕЗОПАСНОСТЬ МЕДИАПРОИЗВОДСТВА. CASE#1: ДОВЕРЕННЫЕ ГРАНИЦЫ МЕЖДУ МЕДИАКОМПЛЕКСАМИ

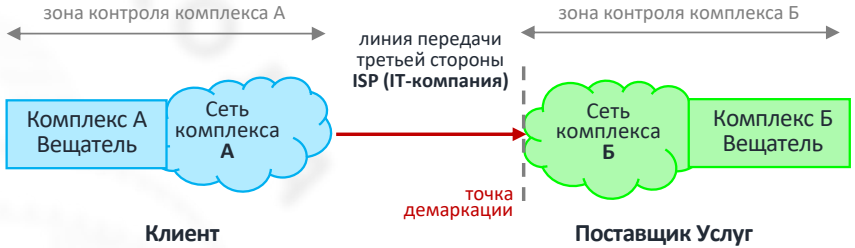
Точка (линия) демаркации – точка разделения ответственности.

IT-индустрия считает:
что Клиент ответственен за подключение к Поставщику услуг;
Вещатели уверены:
что Поставщик услуг отвечает за подключение к Клиенту.

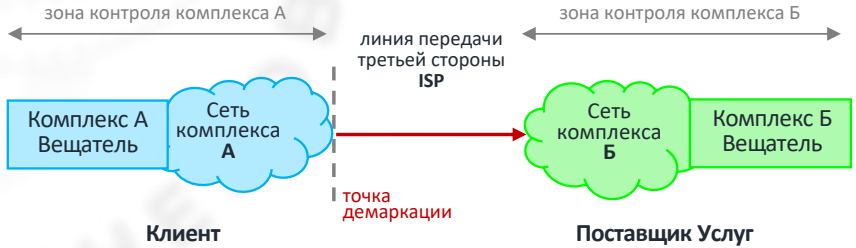
Но кроме разграничения зон ответственности,
не менее важный вопрос – **доверие**:

- между двумя независимыми медиакомпаниями;
- даже между двумя подразделениями одной медиакомпании – никто не рад филиалу, у которого есть «дырка» в своей сети;
- даже внутри медиакомпании: многие рабочие станции (ProTools, Adobe After Effects и др.) требуют прав администратора;
- *и тем более*, между медиакомпанией и поставщиком услуг связи – операторами сетей, ISP, CDN, PTPC и т.д.

А еще есть стыки «производственная сеть – офисная сеть»:
расписания и ресурсы студий и аппаратных, плейлисты, работа с базами данных архивов и доступ к контенту, подготовка новостей…

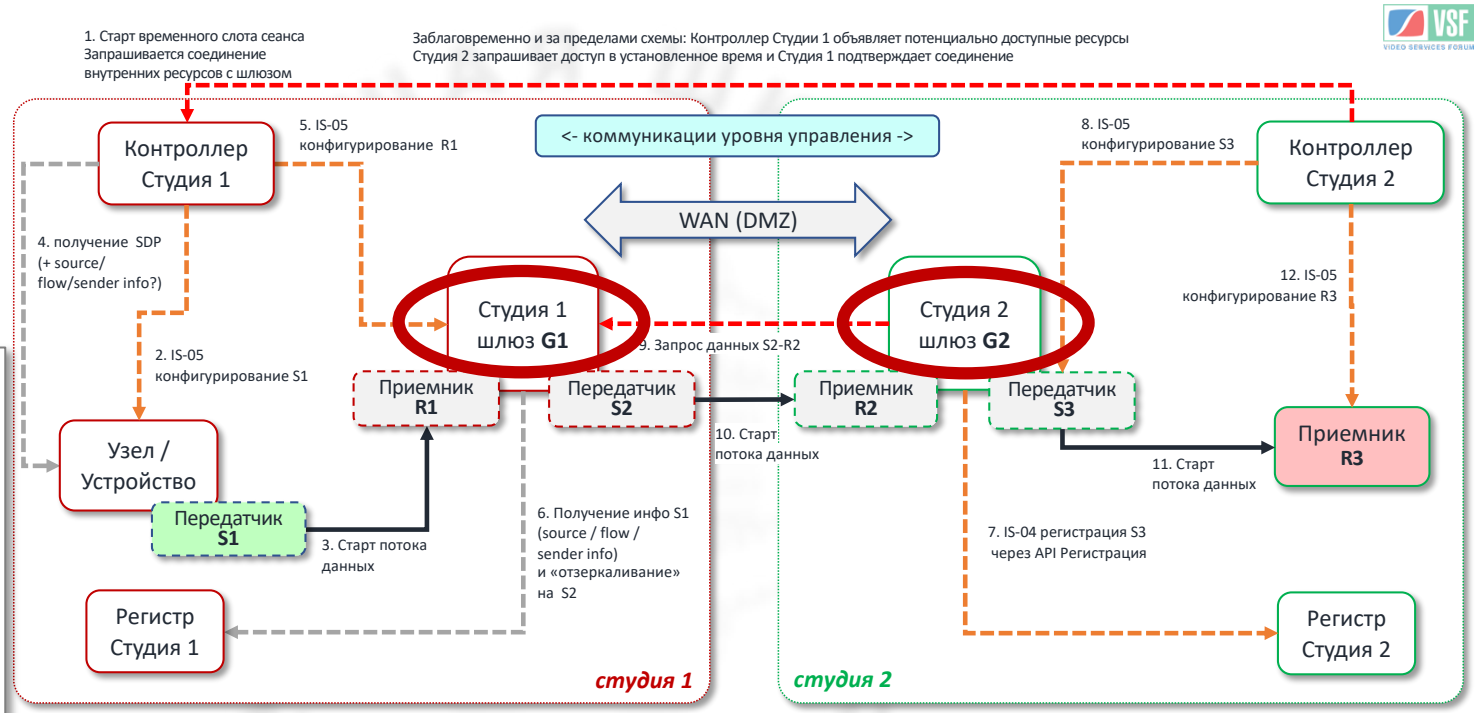


Модель IT-компании



Модель Вещателя

БЕЗОПАСНОСТЬ МЕДИАПРОИЗВОДСТВА. CASE#2: ПЕРЕДАЧА 2110 В СЕТЯХ WAN



Технические рекомендации VSF: решение не только задачи передачи потоков ST 2110,
но и виртуальное соединения уровня управления медиасетями двух подразделений.
Но даже на принципах доверенных интерфейсов не всё так просто: разные подсети, API, сертификатооборот ...

БЕЗОПАСНОСТЬ МЕДИАПРОИЗВОДСТВА. CASE#3: ОБРАЗОВАНИЕ


ПРАВИТЕЛЬСТВО САНКТ-ПЕТЕРБУРГА
КОМИТЕТ ПО ОБРАЗОВАНИЮ

ЛИЦЕНЗИЯ

№ 2949 от 27 июня 2016 г.

на осуществление образовательной деятельности

Настоящая лицензия предоставлена Частному образовательному учреждению

дополнительного профессионального образования

«Высшая школа киноинженеров»

ЧОУ ДПО «Высшая школа киноинженеров»

Частное учреждение

на право оказывать образовательные услуги по реализации образовательных программ по видам образования, по уровням образования, по профессиям, специальностям, направлениям подготовки (для профессионального образования), по подвидам дополнительного образования, указанным в приложении к настоящей лицензии

Основной государственный регистрационный номер юридического лица (индивидуального предпринимателя) (ОГРН) 1137800004372

Идентификационный номер налогоплательщика 7801289796

Серия 78Л02 № 0000881

ШКОЛА ИНЖЕНЕРОВ ТЕЛЕВИДЕНИЯ

ОСНОВАНА В 2017 ГОДУ

WWW.MPE.EDU.RU

ВЫСШАЯ ШКОЛА КИНОИНЖЕНЕРОВ

POWERED BY

Программа повышения квалификации для инженеров телевизионных комплексов и компаний.

онлайн-курс **Передача медиаданных в IP-сетях ТВ-комплексов**

для инженеров и технических руководителей телевизионных компаний

120 часов лекций, самостоятельной работы и тестов без отрыва от производства.

Базовые понятия Media over IP
Основы IP сетей
Протоколы
Компрессия медиаданных
Медиаконтейнеры
Передача медиаданных в IP-сетях
IP-транспорт
Защита контента
Тайминг и синхронизация в IP-сетях
Семейство стандартов SMPTE ST 2022.
Стандарты и спецификации Media over IP. ST 2110
Стандарты и спецификации Media over IP. JT-NM
Стандарты и спецификации Media over IP. NMOS
Технологическая пирамида Media over IP

онлайн
Форма обучения

18 Основные модули

3 Доп. модуля

120 Общее количество часов

9 Часов промежуточных тестов

90 Часов теоретической подготовки

1 Час итоговый тест

20 Часов самостоятельной работы

ВЫСШАЯ ШКОЛА КИНОИНЖЕНЕРОВ

WWW.MPE.EDU.RU

- По итогам прохождения курсов и тестовых заданий обучающимся, имеющим профильное высшее образование выдается Удостоверение о повышении квалификации установленного государственного образца
- Онлайн-оплата для физических лиц либо оплата по счету для организаций
- Безналичная оплата обучения сотрудников от организаций (по договору образовательных услуг)
- NB! Затраты на обучение в целях налогообложения прибыли относятся на себестоимость!