Программа форума

Первый день, 23 апреля

9.00 – 10.00 Регистрация участников. Приветственный кофе
10.00 Торжественное открытие конференции.

Приветственное слово Генерального партнера конференции - **Руслана Рахметова**, генерального директора, ГК «ИНТЕЛЛЕКТУАЛЬНАЯ БЕЗОПАСНОСТЬ», бренд Security Vision

Приветственное слово **Артема Калашникова**, начальника ФИНЦЕРТ Банка России

10.10 – 11.00 ПЛЕНАРНАЯ ДИСКУССИОННАЯ ПАНЕЛЬ: СЦЕНАРИЙ РАЗВИТИЯ КИБЕРБЕЗОПАСНОСТИ: О ЧЕМ ДОЛЖЕН ЗНАТЬ CISO
Зал Секвойя 2+3

Модератор: **Михаил Савельев**, директор по развитию, НИП «ИНФОРМЗАЩИТА»

Вопросы к обсуждению:

- Санкции: на какие средства защиты делать ставку?
- Цифровое средневековье: можно ли выстроить систему защити только на отечественных решениях
- Балканизация интернета: фантазии и реальность

Спикеры:
Андрей Воробьёв, директор, Координационный центр национального домена сети Интернет

Екатерина Митина — продюсер конференции, Тел.: +7 (495) 995-80-04, доб. 1147, e-mail: e.mitina@infor-media.ru Следите за обновлениями на сайте: http://www.infosecurity-forum.ru/
* Организатор не несет ответственности за изменение состава докладчиков и времени их выступления, произошедшие по независящим от организатора причинам.
** Спикер имеет право не предоставлять презентацию своего доклада для общего пользования.

Артем Воробьёв, CISM Information Security Officer CIS GISC Manager Russia Bayer
Максим Наумов, руководитель направления информационной безопасности, СТС Медиа
Илья Сачков, генеральный директор, основатель компании Group-IB
Артем Калашников, начальник ФИНЦЕРТ Банка России
Дмитрий Соломенцев, заместитель руководителя службы защиты инфраструктуры Банка ВТБ
Сергей Гусев, начальник управления информационной безопасности Северсталь

11.00 -12.00 ПЛЕНАРНАЯ ДИСКУССИЯ. Все мы знаем о фундаментальных законах ИБ. Как законодательство меняет подходы по управлению инцидентами

Зал Секвойя 2+3

Модератор: **Алексей Лукацкий**, независимый эксперт

Вопросы к обсуждению:
- Уведомление об инцидентах по требованиям законодательства о безопасности критической инфраструктуры и требованиям Банка России
- Можно ли уведомить об инциденте в течение 3-х часов с момента его обнаружения?
- Обмен информацией об инцидентах
- Базы данных об инцидентах

ОБМЕН ИНФОРМАЦИЕЙ ОБ УГРОЗАХ:
- Стандарты
- Источники
- ГосСОПКА
- ФинЦЕРТ
- Threat Intelligence

Спикеры:
Артем Калашников, начальник ФИНЦЕРТ Банка России
Вячеслав Касимов, начальник управления безопасности, Банк НСПК
Валерий Комаров, специалист по защите информации, отдел методологии информационной безопасности, управление информационной безопасности, Департамент информационных технологий города Москвы
Андрей Курило, председатель Комитета по информационной безопасности НП «Национальный совет финансового рынка»
Василий Окулесский, независимый эксперт
Сергей Пазизин, начальник Управления по обеспечению информационной безопасности ДБ Банка ВТБ
Владимир Скиба, первый заместитель начальника Главного управления информационных технологий ФТС России

Ожидается финальное подтверждение:
Дмитрий Шевцов, начальник управления ФСТЭК России

12.00 – 12.30 Перерыв на кофе, networking

12.30 – 18.00 ЛАЙФХАКИ ДЛЯ ИБ! МАСТЕР-КЛАССЫ, ДИСКУССИИ С ПЕРЧИНКОЙ И ТОП ЛУЧШИХ КЕЙСОВ		
12.30-15.30 БИЗНЕС ПОТОК: Кибербезопасность на языке бизнеса	**12.30-15.30 ТЕХНОЛОГИЧЕСКИЙ ПОТОК: Новые технологии в ИБ: хайп или безлимитище?** **Ноу-хау в области информационной безопасности. Лучшие кейсы и практические рекомендации от ведущих экспертов рынка**	**12.30-13.30 ОРГАНИЗАЦИОННЫЙ ПОТОК: Тонкости службы безопасности**
Зал Секвойя 2	**Зал Секвойя 3**	**Зал Секвойя 4**
Модератор: **Дмитрий Пудов**, технический директор Angara Technologies Group 12.30 – 13.00 Почему важно быть лидером в управлении информационными рисками? И как же ими правильно управлять? - Выгоды управления информационными рисками для компании в целом и для CISO в частности; - Почему многие компании не управляют рисками; - Как эффективно управлять ИБ при ограниченном бюджете; - Мастер-класс: как просто управлять рисками; - Хотите узнать об управлении рисками больше? Где искать информацию? **Федор Горловский**, директор по развитию бизнеса, ГК «ИНТЕЛЛЕКТУАЛЬНАЯ БЕЗОПАСНОСТЬ», бренд Security Vision 13.00-13.30 Кибербезопасность в крупном бизнесе: системный подход: - Современный продовольственный ритейл: риски и ограничения - Комплексный подход к построению периметра кибербезопасности -Вовлечение партнеров в реализацию SOC - Тенденции развития: что будет важно для ритейла в ближайшее время	Модератор: **Павел Крылов,** руководитель направления противодействия онлайн-мошенничеству, Group IB 12.30-12.50 StaffCop Enterpise. Типовые и отраслевые кейсы применения DLP **Дмитрий Кандыбович**, генеральный директор StaffCop 12.50-13.10 Песочные кейсы **Александр Двинских,** эксперт отдела безопасности прикладных систем НИП «ИНФОРМЗАЩИТА» 13.10-13.30 Anti-APT: практика внедрений - Доказательства эффективности использования Anti-APT решений в инфраструктуре заказчика - Примеры по защите почты, веб, файловых хранилищ - Защита рабочих станций нового поколения в составе Anti-APT решений **Александр Русецкий**, руководитель направления по защите от направленных атак Центра информационной безопасности, «Инфосистемы Джет»	12.30-13.00 «Безопасный баланс» при построении ИБ - Какие угрозы сегодня на рынке ИБ? - Что представляет собой злоумышленник? - Что мы делаем сегодня, чтобы завтра за наш взлом платили больше? - Vulnerability management + мотивированный ИТ и ИБ персонал, вот то что нужно для качественной защиты вашей системы - Не один HI TECH в ИБ не победит предателя в ваших рядах, создавая ИБ создавай команду из ИТ и ИБ **Сергей Рысин**, советник директора по безопасности, ПАО государственная транспортная лизинговая компания 13.00-13.30 Как обосновать необходимость ИБ бизнесу? - Продаем страх или защищаем деньги. Как выбрать стратегию? - А сколько стоит опасность? Не стоит запирать сундук на замок, стоящий дороже сундука. - Кто ставит требования, а кто их выполняет. Сервисные функции и «комплекс вахтера». - Не всегда стоит защищать процессы. Понять и сделать их безопасными. **Андрей Коротков**, независимый эксперт

Екатерина Митина — продюсер конференции, Тел.: +7 (495) 995-80-04, доб. 1147, e-mail: e.mitina@infor-media.ru Следите за обновлениями на сайте: http://www.infosecurity-forum.ru/

Андрей Клименко, начальник отдела информационной безопасности и внутреннего аудита, Компания «Лента»		
13.30-14.30 обед		
14.30-15.30 ПРОДОЛЖЕНИЕ БИЗНЕС ПОТОКА: Кибербезопасность на языке бизнеса	**14.30-15.30 ПРОДОЛЖЕНИЕ ТЕХНОЛОГИЧЕСКОГО ПОТОКА: Новые технологии в ИБ: хайп или безлимитище?**	**14.30-15.30 МЕТОДОЛОГИЧЕСКИЙ ПОТОК: ГИБКОСТЬ И AGILE В ЖИЗНИ БЕЗОПАСНИКА**
Зал Секвойя 2	**Зал Секвойя 3**	**Зал Секвойя 4**
14.30-14.50 Аргументация затрат на информационную безопасность: - Как обосновать затраты на развитие информационной безопасности: с чего начать, как аргументировать и к чему стремиться - Уход от классического регулятивного подхода к формированию безопасной среды - Проблемы прямого диалога с высшим руководством в Российских Компаниях по вопросам защиты информации и пути их решения **Александр Севостьянов**, начальник отдела защиты информации СЭБ, ТМК 14.50-15.10 Современное кибероружие. Как защитить себя? **Алексей Плешков,** независимый эксперт по информационной безопасности 15.10-15.30 Аутентификация будущего **Олег Губка,** директор по развитию, Avanpost	14.30-14.50 DocShell — средство автоматизированного управления информационной безопасностью: - текущие проблемы и задачи управления информационной безопасностью в распределенных организациях и ведомствах; - система DocShell как решение этих проблем и задач; - основные функции системы DocShell; - архитектура системы; - опыт и ключевые клиенты — пользователи системы. **Денис Прынков,** директор по маркетингу, «АйТи Мониторинг» 14.50-15.10 Переход в облака - как это сделать безопасно с Aperture **Денис Батранков**, консультант по информационной безопасности, Palo Alto Networks 15.10-15.30 PETYA, МАЙНИНГ, UEBA. Всего лишь хайп или что действительно важно для CISO **Роман Жуков,** руководитель экспертного	Модератор: **Андрей Бажин**, CISO, ВТБ Капитал 14.30-14.50 Управление open source на всех этапах программного проекта -выбор качественных open source компонентов - управление компонентами на этапе сборки ПО - юридическая сторона открытого кода - диалог с безопасностью - а как же сканеры кода? **Гэл Яффе,** региональный директор по странам Европы, Ближнего Востока и Африки, стран азиатско-тихоокеанского региона компании WhiteSource **Elad (Eddie) Tzur,** Director of International Channel Sales at WhiteSource **14.50-15.30 Дискуссия** Вопросы к обсуждению: - Возможен ли Agile в ИБ. Совместимо ли несовместимое? - Когда действительно работает Agile? - Практика применения SCRUM в ИБ - SecDevOps: с чем его едят? Спикеры: **Андрей Акинин,** генеральный директор, Web Control

	направления, **Гарда Технологии** 15.30-15.50 Ахиллесова пята CISO — безопасность бизнес-приложений: разбор наиболее показательных инцидентов, связанных с безопасностью бизнес-приложений (ERP, CRM, CMS): утечки данных, бэкдоры, фрод и др.; почему обеспечение безопасности бизнес-приложений оказывается подчас неразрешимой задачей: логические уязвимости, внутренний нарушитель, непрерывная разработка; что на практике можно предпринять, чтобы минимизировать риски информационной безопасности. **Артур Котылевский,** директор по развитию бизнеса, «Акрибия» 15.50-16.10 Особенности внедрения систем привилегированного доступа в разных организациях **Михаил Романов**, директор по развитию бизнеса, Новые технологии безопасности» (НТБ) 16.10-16.30 тема уточняется Представитель Symantec Corporation	**Илья Борисов**, директор по ИБ «Thyssenkrupp Industrial Solutions» **Андрей Кульпин**, начальник управления защиты ИТ-инфраструктуры, Норильский никель **Андрей Ревяшко**, технический директор, Wildberries **Андрей Шлегель**, менеджер по информационной безопасности, Metro Russia, **Gal Yaffe,** General Manager, EMEA & APAC at WhiteSource **Elad (Eddie) Tzur,** Director of International Channel Sales at WhiteSource
15.30-16.30 ОТКРОВЕННЫЙ РАЗГОВОР: КОМУ ЗА 45+. СТРАТЕГИЯ ВЫХОДА ДЛЯ БЕЗОПАСНИКА. **Зал Секвойя 2** **CISO НА ПЕНСИИ:** Как оно живется в «свободном полете»? Как скопить денег, чтобы жить хорошо на пенсии? Как адаптироваться к мирной жизни и чем заняться после увольнения? Легко ли найти работу сотрудникам в отставке? Как найти работу, если уволили в 45+? Модератор: **Алексей Лукацкий**, независимый эксперт Эксперты: **Василий Окулесский**, независимый эксперт **Рустэм Хайретдинов,** независимый эксперт		**15.30-16.30 КИБЕРУЧЕНИЯ** **Зал Секвойя 4**
16.30 – 17.00 Перерыв на кофе. Голосуй сердцем! Не забудьте отдать свой голос за лучшего спикера форума. Церемония награждения ТОП-10 спикеров состоится 24 апреля в 17.30		

Екатерина Митина — продюсер конференции, Тел.: +7 (495) 995-80-04, доб. 1147, e-mail: e.mitina@infor-media.ru Следите за обновлениями на сайте: http://www.infosecurity-forum.ru/

* Организатор не несет ответственности за изменение состава докладчиков и времени их выступления, произошедшие по независящим от организатора причинам.

** Спикер имеет право не предоставлять презентацию своего доклада для общего пользования.

17.00-18.00 INTELLIGENCE-ПОТОК. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: что идет в комплекте? МАСТЕР-КЛАСС: Риски и возможности новых технологий. Что нового привнесут в жизнь CISO?	17.00-18.00 ПСИХОЛОГИЧЕСКИЙ ПОТОК. Информационная безопасность по Фрейду. МАСТЕР-КЛАСС: Поведенческие паттерны в информационной безопасности	17.00-18.00 КИБЕРУЧЕНИЯ. Продолжение
Зал Секвойя 2	**Зал Секвойя 3**	**Зал Секвойя 4**
Дмитрий Мананников, независимый эксперт Все мы являемся свидетелями 4-й индустриальной революции, в рамках которой мы наблюдаем крайне высокую скорость появления новых технологий. Их уровень проникновения в бизнес крайне высок, риски растут в геометрической прогрессии. И так же растёт разрыв между защищаемыми технологиями и средствами защиты. Последние просто не успевают формироваться, а классические парадигмы вроде периметра защиты уже не работают. Как выстраивать систему защиты в такой среде? Какими качествами должны обладать новые системы защиты? Чем в этом могут помочь большие данные и машинное обучение? И как это все связать воедино на уровне стратегии? Обо всем этом и будем говорить в рамках мастер-класса.	Аномалиями поведения пользователей занимаются довольно давно при проведении расследований: где был, откуда зашёл, что делал до и после инцидента. Однако сегодня, благодаря большому количеству данных и резкому удешевлению инструментов анализа стал возможным переход от пассивной безопасности и расследований к активной защите и даже предсказаниям. В мастер-классе будет представлена теоретическая основа и разбор нескольких практических кейсов. Теоретическая часть: Роль поведенческого анализа в общей структуре безопасности. Где брать данные, какие алгоритмы и инструменты использовать, как строить модели? Как сочетать анализ бизнес-событий (транзакций), поведенческий аналитики (UBA) и коммуникаций (семантический анализ)? Как бороться с ложными срабатываниями? Как перейти от мониторинга к защите через встраивание автоматических контролей? Кейс 1: поведенческий анализ в предсказании уменьшения лояльности Кейс 2: поведенческий анализ в выявлении и блокировании аномалий бизнес-процессов **Рустэм Хайретдинов,** независимый эксперт	

18.00 Завершение официальной программы первого дня форума.

«FuckUp на CISO Forum 2020»

Екатерина Митина — продюсер конференции, Тел.: +7 (495) 995-80-04, доб. 1147, e-mail: e.mitina@infor-media.ru Следите за обновлениями на сайте: http://www.infosecurity-forum.ru/

Мы предлагаем вам «излить душу» - поделиться с участниками форума своими провалами, неуспешными кейсами, проектами, решениями и как вы из них «выпутывались». Себе вы поможете тем, что скинете груз со своих плеч и поймёте, что вы такой не один, а другим – расскажите, как не надо делать и как можно устранить проблему до её появления.

4 главных правила FuckUp:
- говорить не дольше 2х минут
- строго запрещено называть компанию, даже имитировать ее названия
- строго запрещено называть фамилии, должности
- Вам не обязательно предоставлять точные данные, ему нужно донести всю суть провала и какие выводы он сделал

Ведущие:
Алексей Лукацкий, независимый эксперт
Рустэм Хайретдинов, независимый эксперт

День 2, 24 апреля

09.30 – 10.00 Регистрация делегатов.
10.00 – Начало второго дня форума.

10.00 – 11.00 ПЛЕНАРНАЯ ДИСКУССИОННАЯ ПАНЕЛЬ: CISO 2020: ВЗГЛЯД В БУДУЩЕЕ.
Хит-парад ключевых угроз, сильных трендов и многообещающих технологий
Зал Секвойя 2+3

Модератор: **Лев Палей**, начальник отдела обеспечения защиты информации, СО ЕЭС

Вопросы к обсуждению:
- Как изменится роль CISO?
- Как видит бизнес своего CISO?
- Где CISO может получить знание будущего?
- Как развиваются ИТ и бизнес технологии?

Спикеры:
Мона Архипова, директор департамента безопасности и информационных технологий, WayRay
Андрей Акинин, генеральный директор, Web Control
Александр Баранов, заведующий кафедрой информационной безопасности Национального исследовательского университета Высшая Школа Экономики

Сергей Демидов, директор департамента операционных рисков, информационной безопасности и непрерывности рисков, «Московская биржа»
Сергей Ходаков, операционный директор кластера ИТ, Сколково
Алексей Свириденко, начальник управления информационной безопасности, АБ «ИНТЕРПРОГРЕССБАНК»
Лев Шумский, независимый эксперт

УСПЕЙ ПОПАСТЬ В ИСТОРИЮ!
В зоне фойе состоится видео запись коротких интервью участников форума: Успейте попасть в историю и дать свои прогнозы о новых трендах информационной безопасности в России

11.00 – 11.30 Перерыв на кофе

11.30 – 15.40 ДЛЯ ЛЮБИТЕЛЕЙ ОСТРЕНЬКОГО! ДИСКУССИИ С ПЕРЧИНКОЙ И ТОП ЛУЧШИХ КЕЙСОВ		
11.30-13.30 ХАКЕРСКИЙ ПОТОК: О чем знают хакеры, но не знаете вы	**11.30-13.30 ТЕХНОЛОГИЧЕСКИЙ ПОТОК: Защита от современных угроз**	**11.30-13.30 СУДЕБНЫЙ ПОТОК: Тебя посодют, а ты не воруй!**
Зал Секвойя 2	**Зал Секвойя 3**	**Зал Секвойя 4**
Модератор: **Дмитрий Гадарь,** директор департамента информационной безопасности, Tinkoff.ru 11.30-12.30 Автоматизация процессов в SOC/CSIRT командах - Методы работы SOC (Security Operation Center) и CSIRT (computer security incident response team) - Live Response силами команды CSIRT. Как сделать? - Максимальная автоматизация всех рутинных действий (Threat Hunting, Recon, Поиск аномалий и т.д.). **Сергей Серов**, CSIRT Team Lead, «QIWI» 12.30-13.30 Безопасность телеграмм ботов - На сколько вы доверяете данным из мессенджеров? - А насколько самим мессенджерам? - Повсеместные проблемы с авторизацией по	11.30 – 11.50 Мониторинг ИБ: какой SOC вам нужен? **Александр Бодрик,** заместитель генерального директора по развитию бизнеса Angara Professional Assistance 11.50-12.10 Современный подход к управлению уязвимостями С одной стороны, организации уже используют средства, которые сочетают в себе целый комплекс механизмов защиты на разных уровнях. С другой стороны - есть уязвимости, на эксплуатацию которых направлено большинство экплойтов, используемых при проведении атак. Как соединить между собой знания о всех уязвимостях ИТ-инфраструктуры и настроек сетевой безопасности? Как при этом получить полную видимость возможных векторов атак и существенно оптимизировать затраты на эксплуатацию сети и управление уязвимостями? **Юрий Черкас**, территориальный менеджер, Skybox Security, Россия и СНГ	**11.30-12.30 Мастер-класс: Поиски иголки. Судебная практики в области ИТ и ИБ** - Почему почти каждый CISO станет участником гражданского судебного процесса в ближайшее время? - Роль CISO в решение судебных проблем компании. - Личная ответственность и риски CISO. - Самые распространенные группы дел, требующие участия экспертов в области ИТ и ИБ. - Примеры из практики по каждой группе дел. - Важные изменения в практике за 2017-2018 годы. - Что улучшить в своей работе, чтобы избежать правовых последствий? **Евгений Царев,** эксперт по информационной безопасности, судебный эксперт по защите информации, государственная ИТ-безопасность, персональные данные

телефону, некоторые виды атак и типичные ошибки при разработке. **Максим Мошаров**, Application Security Adept, Tinkoff.ru	12.10-12.30 Identity Governance 360°. В чем ценность IDM-решений? Один из самых острых вопросов при наличии большой ИТ-инфраструктуры — как управлять доступом сотрудников (а также сторонних пользователей) к информационным ресурсам компании. - В каких случаях можно задумываться об IdM? - Какие проблемы возникают при отсутствии механизмов централизованного управления доступом? - Как системы IdM могут решить проблемы? **Роман Лунёв,** ведущий менеджер отдела продаж «Газинформсервис» 12.30 – 12.50 Новые способы защиты от «хорошо забытого старого» **Павел Крылов,** руководитель направления противодействия онлайн-мошенничеству, Group IB 12.50-13.10 Защищая самое важное: данные и приложения **Дмитрий Мухтаров,** Security engineer, Imperva	**12.30-13.30 Мастер-класс: DLP при увольнении сотрудников** - Какую роль играют DLP системы при расследовании внутренних инцидентов ИБ? - Какие правовые риски существуют при использовании DLP систем при контроле сотрудников и как их снизить? - Должны ли сотрудники знать об использовании DLP? - Каким правильно регламентировать использование DLP систем? - Как правильно оформлять доказательства собранные DLP системами? - Как использовать DLP с учетом требований GDPR? **Андрей Прозоров,** независимый эксперт
13.30-14.30 обед		
14.30-16.00 ХАКЕРСКИЙ ПОТОК: О чем знают хакеры, но не знаете вы (продолжение)	**14.30-16.00 ЧЕЛОВЕЧЕСКИЙ ФАКТОР В ИБ**	**14.30-16.00 GDPR: практика реализации требований**
Зал Секвойя 2	**Зал Секвойя 3**	**Зал Секвойя 4**
14:30-15:15 Современные реалии предотвращения мошенничества в платёжных системах: анти-фрод в банках - Фрод как новый вид кибер атак на финансовые и платежные системы - Анти-фрод системы и требования	14.30-15.00 Защита от утечки знаний и опыта: неудобные вопросы ИБ, которые можно решить с помощью ML в HR. Опыт и знания - недооценённые информационные активы. Они могут уходить из организации вместе с людьми.	14.30-15.00 GDPR. Что нужно знать российскому бизнесу? - Что регулирует GDPR?; - Применимость GDPR к российским компаниям; - Сравнительный анализ требований GDPR и 152-ФЗ;

регуляторов (СТО БР ИББС, ГОСТ «ФинТех ИБ», П-382, PCI DSS и т.д.) - Технические аспекты фрода или как у нас крадут деньги - Статистика и прогнозы по отрасли - Как работают анти-фрод системы (техническая составляющая) - Технологии в современных анти-фрод системах («классика» и машинное обучение + ИИ) - Типовые кейсы (примеры работы, проблемы, перспективные решения) - Анти-фрод системы в общем ландшафте корпоративных систем обеспечения ИБ - Выводы и прогнозы **Иван Пискунов**, независимый эксперт 15:15 – 16:00 И разработчик станет хакером! Всем известно, что автоматизация контролей и процессов безопасности — это один из основных ответов безопасности на вызов постоянно ускоряющегося цикла разработки. При этом очевидно, хотя и утопично, что было бы здорово писать безопасный код изначально. Что бы это стало возможным, безопасность должна присутствовать в жизни разработчика с первых дней его работы, с первых строчек кода. В докладе разберём практические сценарии и опыт повышения уровня культуры безопасности в современной интернет-компании. **Тарас Иващенко,** независимый эксперт	Когда это происходит, это трудно предотвратить, хорошо работает только профилактика. Меры по профилактике ухода лучших сотрудников вместе с их знаниями и опытом стоят дорого и в основном их можно себе позволить только точечно. С помощью ML, можно учить модели, которые прогнозируют действия сотрудников, которые уже работают, в том числе изменение KPI и уход. Но лучше сразу нанимать с помощью этих моделей тех, у кого будут лучшие KPI, и кто проработает дольше. **Александр Сидоров**, руководитель направления анализа данных, HeadHunter 15.00-15.30 Построение ИБ-культуры. Обучение и повышение осведомленности сотрудников и методы социальной инженерии **Лев Палей**, начальник отдела обеспечения защиты информации, СО ЕЭС 15.30-16.00 Человек - и есть главная угроза информационной безопасности. Но если ему дать знания и обучение, то это позволит снизить угрозу. Давайте поймем как? **Дмитрий Костров**, независимый эксперт	- Последствия несоблюдения требований. **Дмитрий Бирюков**, менеджер, отдел анализа и контроля рисков, PwC **Артём Дмитриев**, старший юрист практики по интеллектуальной собственности, технологиям и защите данных, PwC Legal 15.00-15.30 GDPR: практика реализации требований - Анализ практики и подходов к реализации требований в организациях: - Вовлеченность руководства - Роли и ответственность - Распределение задач и вовлеченность подразделений - Методологии и инструменты внедрения требований GDPR - Рекомендации по организации реализации требований. **Константин Коротнев**, старший менеджер, отдел анализа и контроля рисков, PwC **15.30-16.00 Секция вопросов и ответов по теме GDPR** **Константин Коротнев,** старший менеджер, отдел анализа и контроля рисков, PwC **Дмитрий Бирюков**, менеджер, отдел анализа и контроля рисков, PwC **Артём Дмитриев**, старший юрист практики по интеллектуальной собственности, технологиям и защите данных, PwC Legal

16.00-16.30 Перерыв на кофе

Екатерина Митина — продюсер конференции, Тел.: +7 (495) 995-80-04, доб. 1147, e-mail: e.mitina@infor-media.ru Следите за обновлениями на сайте: http://www.infosecurity-forum.ru/

16.30 – 17.30 Мастер-класс. **Вы построили SOC, что дальше?**	**16.30-17.30 Мастер-класс.** **Дашборды по ИБ: как визуализировать кибербезопасность для руководства**	**16.30-17.30 Мастер-класс.** **Базы уязвимостей. Изводя тысячи тонн словесной руды.**
Зал Секвойя 2	**Зал Секвойя 3**	**Зал Секвойя 4**
- Оптимизации операционных задач, - Превращения «обычного» MSSP в «продвинутого» - Голубые, красные и пурпурные команды - Операционная работа как источник Threat Intelligence **Сергей Солдатов**, независимый эксперт	- Как должен выглядеть отчет/дашборд по ИБ для руководства? - Кто вы и ваша целевая аудитория? - Кто ваш заказчик? - Кто будет смотреть на ваш отчет или дашборд? - Что нужно вашей целевой аудитории? - Какие ключевые показатели ей необходимо показать? - Какое решение должна принять ваша целевая аудитория? - Могут ли ваши дашборды/отчеты помочь ответить на вопросы, волнующие бизнес? **Алексей Лукацкий,** независимый эксперт	- Проблемы формализации данных об уязвимостях: кто-то где-то что-то нашел - Детектирование уязвимостей по руке и на кофейной гуще - Видишь эксплоит? Нет. А он есть! Или нет. - Пока гром не грянет, мужик не просканит. - Трагикомедия чипапокалипсиса: не спеши выполнять — отменят - Лишение сертификатов за неисправленные уязвимости. Плюсы и минусы. **Александр Леонов**, старший аналитик по информационной безопасности «Тинькофф Банк»

17.30 ИМПЕРИЯ СИЛЬНЕЙШИХ!
Парад спикеров. Подведение итогов голосования за лучших спикеров форума. Рейтинг спикеров и церемония награждения ТОП – 10!

18.00 Завершение конференции.

Екатерина Митина — продюсер конференции, Тел.: +7 (495) 995-80-04, доб. 1147, e-mail: e.mitina@infor-media.ru Следите за обновлениями на сайте: http://www.infosecurity-forum.ru/