



### 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 защиты только на отечественных решениях
- Балканизация интернета: фантазии и реальность

#### Спикеры:

**Артем Воробьев**, CISM Information Security Officer CIS GISC Manager Russia Bayer

**Екатерина Митина** — продюсер конференции, Тел.: +7 (495) 995-80-04, доб. 1147, e-mail: [e.mitina@infor-media.ru](mailto: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.

**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

**Константин Коротнев**, старший менеджер, отдел анализа и контроля рисков, PwC

## 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

**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

12.00 – 12.30 Перерыв на кофе, networking

Екатерина Митина — продюсер конференции, Тел.: +7 (495) 995-80-04, доб. 1147, e-mail: [e.mitina@infor-media.ru](mailto: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.

**12.30 – 18.00 ЛАЙФХАКИ ДЛЯ ИБ! МАСТЕР-КЛАССЫ, ДИСКУССИИ С ПЕРЧИНКОЙ И ТОП ЛУЧШИХ КЕЙСОВ**

<p><b>12.30-15.30 БИЗНЕС ПОТОК:</b> Кибербезопасность на языке бизнеса</p>	<p><b>12.30-15.30 ТЕХНОЛОГИЧЕСКИЙ ПОТОК:</b> Новые технологии в ИБ: хайп или безлимитище?</p> <p>Ноу-хау в области информационной безопасности. Лучшие кейсы и практические рекомендации от ведущих экспертов рынка</p>	<p><b>12.30-13.30 ОРГАНИЗАЦИОННЫЙ ПОТОК:</b> Тонкости службы безопасности</p>
<p><b>Зал Секвойя 2</b></p>	<p><b>Зал Секвойя 3</b></p>	<p><b>Зал Секвойя 4</b></p>
<p>Модератор: <b>Дмитрий Пудов</b>, технический директор Angara Technologies Group</p> <p>12.30 – 13.00 Почему важно быть лидером в управлении информационными рисками? И как же ими правильно управлять?</p> <ul style="list-style-type: none"> <li>- Выгоды управления информационными рисками для компании в целом и для CISO в частности;</li> <li>- Почему многие компании не управляют рисками;</li> <li>- Как эффективно управлять ИБ при ограниченном бюджете;</li> <li>- Мастер-класс: как просто управлять рисками;</li> <li>- Хотите узнать об управлении рисками больше? Где искать информацию?</li> </ul> <p><b>Федор Горловский</b>, директор по развитию бизнеса, ГК «ИНТЕЛЛЕКТУАЛЬНАЯ БЕЗОПАСНОСТЬ», бренд Security Vision</p> <p>13.00-13.30 Кибербезопасность в крупном бизнесе: системный подход:</p> <ul style="list-style-type: none"> <li>- Современный продовольственный ритейл: риски и ограничения</li> <li>- Комплексный подход к построению периметра кибербезопасности</li> <li>- Вовлечение партнеров в реализацию SOC</li> <li>- Тенденции развития: что будет важно для ритейла в ближайшее время</li> </ul> <p><b>Андрей Клименко</b>, начальник отдела информационной безопасности и внутреннего</p>	<p>Модератор: <b>Павел Крылов</b>, руководитель направления противодействия онлайн-мошенничеству, Group IB</p> <p>12.30-12.50 StaffCop Enterprise. Типовые и отраслевые кейсы применения DLP <b>Дмитрий Кандыбович</b>, генеральный директор StaffCop</p> <p>12.50-13.10 Песочные кейсы <b>Александр Двинских</b>, эксперт отдела безопасности прикладных систем НИП «ИНФОРМЗАЩИТА»</p> <p>13.10-13.30 Anti-APT: практика внедрений</p> <ul style="list-style-type: none"> <li>- Доказательства эффективности использования Anti-APT решений в инфраструктуре заказчика</li> <li>- Примеры по защите почты, веб, файловых хранилищ</li> <li>- Защита рабочих станций нового поколения в составе Anti-APT решений</li> </ul> <p><b>Александр Русецкий</b>, руководитель направления по защите от направленных атак Центра информационной безопасности, «Инфосистемы Джет»</p>	<p>12.30-13.00 «Безопасный баланс» при построении ИБ</p> <ul style="list-style-type: none"> <li>- Какие угрозы сегодня на рынке ИБ?</li> <li>- Что представляет собой злоумышленник?</li> <li>- Что мы делаем сегодня, чтобы завтра за наш взлом платили больше?</li> <li>- Vulnerability management + мотивированный ИТ и ИБ персонал, вот то что нужно для качественной защиты вашей системы</li> <li>- Не один HI TECH в ИБ не победит предателя в ваших рядах, создавая ИБ создавай команду из ИТ и ИБ</li> </ul> <p><b>Сергей Рысин</b>, советник директора по безопасности, ПАО государственная транспортная лизинговая компания</p> <p>13.00-13.30 Как обосновать необходимость ИБ бизнесу?</p> <ul style="list-style-type: none"> <li>- Продаем страх или защищаем деньги. Как выбрать стратегию?</li> <li>- А сколько стоит опасность? Не стоит запираеть сундук на замок, стоящий дороже сундука.</li> <li>- Кто ставит требования, а кто их выполняет. Сервисные функции и «комплекс вахтера».</li> <li>- Не всегда стоит защищать процессы. Понять и сделать их безопасными.</li> </ul> <p><b>Андрей Коротков</b>, независимый эксперт</p>

Екатерина Митина — продюсер конференции, Тел.: +7 (495) 995-80-04, доб. 1147, e-mail: [e.mitina@infor-media.ru](mailto: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.

аудита, Компания «Лента»		
<b>13.30-14.30 обед</b>		
<b>14.30-15.30 ПРОДОЛЖЕНИЕ БИЗНЕС ПОТОКА: Кибербезопасность на языке бизнеса</b>	<b>14.30-15.30 ПРОДОЛЖЕНИЕ ТЕХНОЛОГИЧЕСКОГО ПОТОКА: Новые технологии в ИБ: хайп или безлимитище?</b>	<b>14.30-15.30 МЕТОДОЛОГИЧЕСКИЙ ПОТОК: ГИБКОСТЬ И AGILE В ЖИЗНИ БЕЗОПАСНИКА</b>
<b>Зал Секвойя 2</b>	<b>Зал Секвойя 3</b>	<b>Зал Секвойя 4</b>
<p>14.30-14.50 Аргументация затрат на информационную безопасность:</p> <ul style="list-style-type: none"> <li>- Как обосновать затраты на развитие информационной безопасности: с чего начать, как аргументировать и к чему стремиться</li> <li>- Уход от классического регулятивного подхода к формированию безопасной среды</li> <li>- Проблемы прямого диалога с высшим руководством в Российских Компаниях по вопросам защиты информации и пути их решения</li> </ul> <p><b>Александр Севостьянов</b>, начальник отдела защиты информации СЭБ, ТМК</p> <p>14.50-15.10 Современное кибероружие. Как защитить себя?</p> <p><b>Алексей Плешков</b>, независимый эксперт по информационной безопасности</p> <p>15.10-15.30 Аутентификация будущего</p> <p><b>Олег Губка</b>, директор по развитию, Avanpost</p>	<p>14.30-14.50 DocShell — средство автоматизированного управления информационной безопасностью:</p> <ul style="list-style-type: none"> <li>- текущие проблемы и задачи управления информационной безопасностью в распределенных организациях и ведомствах;</li> <li>- система DocShell как решение этих проблем и задач;</li> <li>- основные функции системы DocShell;</li> <li>- архитектура системы;</li> <li>- опыт и ключевые клиенты — пользователи системы.</li> </ul> <p><b>Денис Прынков</b>, директор по маркетингу, «АйТи Мониторинг»</p> <p>14.50-15.10 Переход в облака - как это сделать безопасно с Aperture</p> <p><b>Денис Батранков</b>, консультант по информационной безопасности, Palo Alto Networks</p> <p>15.10-15.30 РЕТУА, МАЙНИНГ, UEBA. Всего лишь хайп или что действительно важно для CISO</p> <p><b>Роман Жуков</b>, руководитель экспертного</p>	<p>Модератор: <b>Андрей Бажин</b>, CISO, ВТБ Капитал</p> <p>14.30-14.50 Управление open source на всех этапах программного проекта</p> <ul style="list-style-type: none"> <li>- выбор качественных open source компонентов</li> <li>- управление компонентами на этапе сборки ПО</li> <li>- юридическая сторона открытого кода</li> <li>- диалог с безопасностью</li> <li>- а как же сканеры кода?</li> </ul> <p><b>Гэл Яффе</b>, региональный директор по странам Европы, Ближнего Востока и Африки, стран азиатско-тихоокеанского региона компании WhiteSource</p> <p><b>Elad (Eddie) Tzur</b>, Director of International Channel Sales at WhiteSource</p> <p><b>14.50-15.30 Дискуссия</b></p> <p>Вопросы к обсуждению:</p> <ul style="list-style-type: none"> <li>- Возможен ли Agile в ИБ. Совместимо ли несовместимое?</li> <li>- Когда действительно работает Agile?</li> <li>- Практика применения SCRUM в ИБ</li> <li>- SecDevOps: с чем его едят?</li> </ul> <p>Спикеры:</p> <p><b>Андрей Акинин</b>, генеральный директор, Web Control</p>

Екатерина Митина — продюсер конференции, Тел.: +7 (495) 995-80-04, доб. 1147, e-mail: [e.mitina@infor-media.ru](mailto: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.

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

Екатерина Митина — продюсер конференции, Тел.: +7 (495) 995-80-04, доб. 1147, e-mail: [e.mitina@infor-media.ru](mailto: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.

<p><b>17.00-18.00 INTELLIGENCE-ПОТОК.</b>  <b>ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: что идет в комплекте?</b>  <b>МАСТЕР-КЛАСС: Риски и возможности новых технологий. Что нового принесут в жизнь CISO?</b></p>	<p><b>17.00-18.00 ПСИХОЛОГИЧЕСКИЙ ПОТОК.</b>  <b>Информационная безопасность по Фрейду.</b>  <b>МАСТЕР-КЛАСС: Поведенческие паттерны в информационной безопасности</b></p>	
<p><b>Зал Секвойя 2</b></p>	<p><b>Зал Секвойя 3</b></p>	
<p><b>Дмитрий Мананников</b>, независимый эксперт</p> <p>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.</p>	<p>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.</p> <p>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), поведенческой аналитики (UBA) и коммуникаций (семантический анализ)? Как бороться с ложными срабатываниями? Как перейти от мониторинга к защите через встраивание автоматических контролей?</p> <p>Кейс 1: поведенческий анализ в предсказании уменьшения лояльности</p> <p>Кейс 2: поведенческий анализ в выявлении и блокировании аномалий бизнес-процессов</p> <p><b>Рустэм Хайретдинов</b>, независимый эксперт</p>	

**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](mailto: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.

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

Екатерина Митина — продюсер конференции, Тел.: +7 (495) 995-80-04, доб. 1147, e-mail: [e.mitina@infor-media.ru](mailto: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.

**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 посадят, а ты не воруй!
Зал Секвойя 2	Зал Секвойя 3	Зал Секвойя 4
<p>Модератор: <b>Дмитрий Гадарь</b>, директор департамента информационной безопасности, Tinkoff.ru</p> <p>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.).  <b>Сергей Серов</b>, CSIRT Team Lead, «QIWI»</p> <p>12.30-13.30 Безопасность телеграмм ботов            - На сколько вы доверяете данным из мессенджеров?            - А насколько самим мессенджерам?            - Повсеместные проблемы с авторизацией по</p>	<p>11.30 – 11.50 Мониторинг ИБ: какой SOC вам нужен?  <b>Александр Бодрик</b>, заместитель генерального директора по развитию бизнеса Angara Professional Assistance</p> <p>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 эксплойтов, 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?  <b>Юрий Черкас</b>, территориальный менеджер, Skybox Security, Россия и СНГ</p>	<p><b>11.30-12.30 Мастер-класс: Поиски иголки. Судебная практики в области ИТ и ИБ</b></p> <ul style="list-style-type: none"> <li>- Почему почти каждый CISO станет участником гражданского судебного процесса в ближайшее время?</li> <li>- Роль CISO в решение судебных проблем компании.</li> <li>- Личная ответственность и риски CISO.</li> <li>- Самые распространенные группы дел, требующие участия экспертов в области ИТ и ИБ.</li> <li>- Примеры из практики по каждой группе дел.</li> <li>- Важные изменения в практике за 2017-2018 годы.</li> <li>- Что улучшить в своей работе, чтобы избежать правовых последствий?</li> </ul> <p><b>Евгений Царев</b>, эксперт по информационной безопасности, судебный эксперт по защите информации, государственная ИТ-безопасность, персональные данные</p>

Екатерина Митина — продюсер конференции, Тел.: +7 (495) 995-80-04, доб. 1147, e-mail: [e.mitina@infor-media.ru](mailto: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.

<p>телефону, некоторые виды атак и типичные ошибки при разработке.  <b>Максим Мошаров</b>, Application Security Adept, Tinkoff.ru</p>	<p>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?  <b>Роман Лунёв</b>, ведущий менеджер отдела продаж «Газинформсервис»</p> <p>12.30 – 12.50 Новые способы защиты от «хорошо забытого старого»  <b>Павел Крылов</b>, руководитель направления противодействия онлайн-мошенничеству, Group IB</p> <p>12.50-13.10 Защищая самое важное: данные и приложения  <b>Дмитрий Мухтаров</b>, Security engineer, Imperva</p> <p>13.10-13.30 Symantec Web Isolation: изолированная среда для безопасности доступа сотрудников в интернет  <b>Олег Никитский</b>, региональный менеджер, Symantec Russia and CIS</p>	<p><b>12.30-13.30 Мастер-класс: DLP при увольнении сотрудников</b>  - 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?  <b>Андрей Прозоров</b>, независимый эксперт</p>
---	--	--

<p><b>13.30-14.30 обед</b></p>		
<p><b>14.30-16.00 ХАКЕРСКИЙ ПОТОК: О чем знают хакеры, но не знаете вы (продолжение)</b></p>	<p><b>14.30-16.00 ЧЕЛОВЕЧЕСКИЙ ФАКТОР В ИБ</b></p>	<p><b>14.30-16.00 GDPR: практика реализации требований</b></p>
<p><b>Зал Секвойя 2</b></p>	<p><b>Зал Секвойя 3</b></p>	<p><b>Зал Секвойя 4</b></p>
<p>14:30-15:15 Современные реалии</p>	<p>14.30-15.00 Защита от утечки знаний и опыта:</p>	<p>14.30-15.00 GDPR. Что нужно знать российскому</p>

Екатерина Митина — продюсер конференции, Тел.: +7 (495) 995-80-04, доб. 1147, e-mail: [e.mitina@infor-media.ru](mailto: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.

<p>предотвращения мошенничества в платёжных системах: анти-фрод в банках</p> <ul style="list-style-type: none"> <li>- Фрод как новый вид кибер атак на финансовые и платежные системы</li> <li>- Анти-фрод системы и требования регуляторов (СТО БР ИББС, ГОСТ «ФинТех ИБ», П-382, PCI DSS и т.д.)</li> <li>- Технические аспекты фрода или как у нас крадут деньги</li> <li>- Статистика и прогнозы по отрасли</li> <li>- Как работают анти-фрод системы (техническая составляющая)</li> <li>- Технологии в современных анти-фрод системах («классика» и машинное обучение + ИИ)</li> <li>- Типовые кейсы (примеры работы, проблемы, перспективные решения)</li> <li>- Анти-фрод системы в общем ландшафте корпоративных систем обеспечения ИБ</li> <li>- Выводы и прогнозы</li> </ul> <p><b>Иван Пискунов</b>, независимый эксперт</p> <p>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-компани.</p> <p><b>Тарас Иващенко</b>, независимый эксперт</p>	<p>неудобные вопросы ИБ, которые можно решить с помощью ML в HR.</p> <p>Опыт и знания - недооценённые информационные активы. Они могут уходить из организации вместе с людьми.</p> <p>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 точно.</p> <p>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.</p> <p><b>Александр Сидоров</b>, руководитель направления анализа данных, HeadHunter</p> <p>15.00-15.30 Построение ИБ-культуры. Обучение и повышение осведомленности сотрудников и методы социальной инженерии</p> <p><b>Лев Палей</b>, начальник отдела обеспечения защиты информации, СО ЕЭС</p> <p>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?</p> <p><b>Дмитрий Костров</b>, независимый эксперт</p>	<p>бизнесу?</p> <ul style="list-style-type: none"> <li>- Что регулирует GDPR?;</li> <li>- Применимость GDPR к российским компаниям;</li> <li>- Сравнительный анализ требований GDPR и 152-ФЗ;</li> <li>- Последствия несоблюдения требований.</li> </ul> <p><b>Дмитрий Бирюков</b>, менеджер, отдел анализа и контроля рисков, PwC</p> <p><b>Артём Дмитриев</b>, старший юрист практики по интеллектуальной собственности, технологиям и защите данных, PwC Legal</p> <p>15.00-15.30 GDPR: практика реализации требований</p> <ul style="list-style-type: none"> <li>- Анализ практики и подходов к реализации требований в организациях:</li> <li>- Вовлеченность руководства</li> <li>- Роли и ответственность</li> <li>- Распределение задач и вовлеченность подразделений</li> <li>- Методологии и инструменты внедрения требований GDPR</li> <li>- Рекомендации по организации реализации требований.</li> </ul> <p><b>Константин Коротнев</b>, старший менеджер, отдел анализа и контроля рисков, PwC</p> <p><b>15.30-16.00 Секция вопросов и ответов по теме GDPR</b></p> <p><b>Константин Коротнев</b>, старший менеджер, отдел анализа и контроля рисков, PwC</p> <p><b>Дмитрий Бирюков</b>, менеджер, отдел анализа и контроля рисков, PwC</p> <p><b>Артём Дмитриев</b>, старший юрист практики по интеллектуальной собственности, технологиям и</p>
---	---	--

**16.00-16.30 Перерыв на кофе**

<b>16.30-17.30 Мастер-класс.</b> <b>Дашборды по ИБ: как визуализировать кибербезопасность для руководства</b>	<b>16.30-17.30 Мастер-класс.</b> <b>Базы уязвимостей. Изводя тысячи тонн словесной руды.</b>
<b>Зал Секвойя 3</b>	<b>Зал Секвойя 4</b>
<ul style="list-style-type: none"> <li>- Как должен выглядеть отчет/дашборд по ИБ для руководства?</li> <li>- Кто вы и ваша целевая аудитория?</li> <li>- Кто ваш заказчик?</li> <li>- Кто будет смотреть на ваш отчет или дашборд?</li> <li>- Что нужно вашей целевой аудитории?</li> <li>- Какие ключевые показатели ей необходимо показать?</li> <li>- Какое решение должна принять ваша целевая аудитория?</li> <li>- Могут ли ваши дашборды/отчеты помочь ответить на вопросы, волнующие бизнес?</li> </ul> <p><b>Алексей Лукацкий</b>, независимый эксперт</p>	<ul style="list-style-type: none"> <li>- Проблемы формализации данных об уязвимостях: кто-то где-то что-то нашел</li> <li>- Детектирование уязвимостей по руке и на кофейной гуще</li> <li>- Видишь эксплоит? Нет. А он есть! Или нет.</li> <li>- Пока гром не грянет, мужик не просканит.</li> <li>- Трагикомедия чипапокалипсиса: не спеши выполнять — отменят</li> <li>- Лишение сертификатов за неисправленные уязвимости. Плюсы и минусы.</li> </ul> <p><b>Александр Леонов</b>, старший аналитик по информационной безопасности «Тинькофф Банк»</p>

**17.30 ИМПЕРИЯ СИЛЬНЕЙШИХ!**

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

**18.00 Завершение конференции.**