Старейший актуальный

Хроники XXIII Международного форума «Технологии безопасности»

С 13 по 15 февраля 2018 года в Москве прошел XXIII Международный форум «Технологии безопасности». К мощной деловой программе организаторы главного GR-форума отрасли добавили важный элемент — предварительные, в течение года, встречи бизнеса с госзаказчиками. В результате на конференциях ТБ Форума спикеры и аудитория значительно лучше понимали друг друга при обсуждении таких тем, как безопасность спортивных объектов, транспортных и энергетических предприятий, построение сегментов «Безопасного города».

Текст: Римма Ремизова, Станислав Тарасов

В ПЛОТНЫХ СЛОЯХ КОНКУРЕНТНОЙ АТМОСФЕРЫ

ТБ Форуму уже 23 года — мероприятие с историей, в этом есть свое преимущество, но есть и риски. В 2018 году организаторам из компании «Гротек» пришлось выдержать серьезную конкуренцию с целым набором альтернативных форматов бизнес-коммуникаций.

Всего за год-полтора рынок безопасности с головой окунулся в интернет-сервисы: вебинары, видеоконференции; чаты и тематические группы в мессенджерах стали повседневной средой общения специалистов. Они, конечно, не могут заменить живого общения с коллегами и заказчиками, но с ежегодным форумом в скорости обратной связи не сравнятся.

При этом не ослабла конкуренция в офлайне. Многие ведомства — в первую очередь силовики уровня МВД, Росгвардии, Минобороны — закрепили за собой профильные выставочно-форумные площадки (Научно-технический форум «День передовых технологий правоохранительных органов Российской Федерации» проходит в мае на полигоне в Балашихе, а в августе на территории парка «Патриот» в Кубинке развернет свою работу «Неделя национальной безопасности» — и это будет только часть глобального форума «Армия», проходящего там же и в то же время).

Кроме того, границы мероприятий для рынка систем безопасности размыли коллеги из смежных отраслей. Все чаще на них можно увидеть имена и логотипы, происходящие из сегмента технических средств безопасности. Почти накануне ТБ Форума в «Крокус Экспо» прошла Национальная выставка инфраструктуры гражданской авиации NAIS-2018 (спонсорами секции «Безопасность» выступили Nuctech, Центр Речевых Технологий и интегратор КРОК, среди 29 производителей решения по безопасности были Wekey, ООО «Диагностика-М», ЗАО «НПЦ «Аспект», ООО «НЕОСКАН», ООО «Пожарная автоматика»). Тему безопасности активно использовали в своей повестке крупные государственные форумы — «Российская энергетическая неделя» (среди спикеров — ООО «НПФ Видар», груп-

The oldest is the hotest / By Rimma Remizova, Stanislav Tarasov

XXIII International Forum «Security and Safety Technologies» was held from 13-15 February in Moscow. To the powerful business program, organizers of the main GR-forum in the industry added an important element — preliminary (during the year) business meetings with state customers. As a result, at the conferences of the ST Forum, speakers and the audience understood each other much better when discussing topics such as the safety of sports facilities, transport and energy enterprises, and the construction of «Safe city» segments.

па компаний «Стилсофт», Schneider Electric) и «Транспорт России» в рамках Транспортной недели (отдельная панельная сессия по транспортной безопасности, модератором которой выступил лично замминистра Николай Захряпин).

Впрочем, «Гротек» правильно сориентировался по ситуации и запустил собственный формат — закрытые встречи производителей с госзаказчиками. Встречи подавались строго в связи с ТБ Форумом (для его участников), проходили в атмосфере секретности и по личному отбору организаторов в течение всего 2017 года. Понятно, что интерес тех, кто не был приглашен на «тайные вечери», подогревала возможность попасть хотя бы на открытые выступления лиц, принимающих решения о закупках и поставках оборудования в государственный сектор.

В деловой программе — 12 мероприятий; 226 спикеров: регуляторы, крупнейшие заказчики, разработчики, эксперты; на 30% выше предварительная регистрация посетителей и делегатов.

ПОРТРЕТНАЯ ГАЛЕРЕЯ

Торжественная церемония открытия форума ожидаемо прошла при аншлаге. По составу президиума посетители еще до старта определяют обычно степень интереса к форуму со стороны потенциальных заказчиков и государственных ведомств. Ожидания оправдались, интерес по-прежнему есть. Наравне с новым председателем оргкомитета **Виктором Бондаревым** (сменил на этом посту сенатора Виктора Озерова) собравшихся приветствовали член комитета Государственной Думы по безопасности и противодействию коррупции **Дмитрий Перминов**, заместитель руководителя Антитеррористического центра государств-участников СНГ Сергей Дудко, председатель Комиссии Московской городской Думы по безопасности **Инна Святенко**, депутат, член комитета по транспорту и строительству Госдумы **Александр Старовойтов**.

Делегатом от бизнеса среди государственников стал заместитель генерального директора АО «Астерос» **Владимир Шелепов**, он даже получил статуэтку Малого ЗУБРа (брендированная награда от организаторов) — «За укрепление безопасности России». Правда, по досадному стечению обстоятельств тогдашний работодатель Владимира на момент написания этого материала заявил о прекращении деятельности и запустил процедуру банкротства. Так что статуэтка от ТБ Форума станет для топ-менеджера «Астерос» особенно памятной.

Ключевые участники ТБ Форума-2018

1. **Группа «Астерос»** — стенд; комплексные системы безопасности и антитеррористической защиты

Генеральный партнер темы конференции «Безопасность спортивных и массовых мероприятий»

Деловая программа:

- *«Практические аспекты обеспечения безопасности и антитеррористической защиты спортивных объектов и прилегающей территории»;*
- *«Ключевые аспекты обеспечения безопасности массовых мероприятий. Вызовы для государства и участников рынка».*

2. **«Артсок»** — стенд; разработка и производство средств газового пожаротушения

3. **«БайтЭрг»** — стенд; российский производитель видеокамер

4. **«Газинформсервис»** — стенд; системный интегратор, системы информационной безопасности

5. **Завод «Егоза»** — стенд; производитель средств физической защиты периметра

6. **«ВЛИБОР Системс»** — стенд; системы досмотра и антитеррористической защиты

Деловая программа:

- *«Комплексная защита объектов солнечной энергетики»*

7. **«Джи-Эм-Пи-РуссКом»** — стенд; оборудование и расходные материалы для производства пластиковых карт

Деловая программа:

- *«Защищенные документы в формате пластиковых карт. Способы продления срока службы и защита от копирования и подделки»*

8. **Инновационный центр безопасности** — информационная и комплексная безопасность

Коспонсор конференции «SecuFinance: защитные технологии банка будущего»

Деловая программа:

- *«Использование многоуровневого анализа голоса в целях обеспечения комплексной безопасности»;*
- *«Угрозы от бесконтрольного применения БПЛА. Способы их устранения за счет применения мультисенсорных систем обнаружения и «подавления».*

9. **«Интегра-С»** — стенд; интеллектуальные интегрированные системы безопасности

Деловая программа:

- *«Система непрерывного мониторинга ситуаций на объектах транспорта. Опыт внедрения»;*
- *«ИНТЕГРА-ПЛАНЕТА-4D» как основа «Цифровой России» и готовое решение для АПК «Безопасный город»;*
- *«Единая интеграционная платформа для обеспечения комплексной безопасности объектов промышленности, нефтегаза и энергетики. Опыт внедрения»;*
- *«Необходимость построения единой системы непрерывного мониторинга ситуаций на объектах ЧМ-2018».*

10. **Институт инженерной физики**

Деловая программа:

- *«Охранные извещатели серии TRAVERS. Особенности. Преимущества. Практика применения»;*
- *«Комплексная система обеспечения безопасности объектов и территорий «Ловец». Наш взгляд в будущее».*

11. **Код безопасности** — стенд; системы информационной безопасности

Сопартнер конференции «Актуальные вопросы защиты информации»

12. **ГК «Конфидент»** — системы информационной безопасности

Партнер конференции «Актуальные вопросы защиты информации»

Деловая программа:

- *«Устранение уязвимостей в сертифицированных средствах защиты информации. Опыт российского разработчика и анализ ситуации в проектах по информационной безопасности».*

13. **КРОК**

Коспонсор конференции «SecuRetail: комплексная безопасность торговых центров и ритейла»

Деловая программа:

- *«Системная интеграция — эффективный ответ на современные угрозы безопасности»;*
- *«Использование беспилотников в рамках ситуационных и командных центров»;*
- *«Больше, чем видео: повышение эффективности бизнеса и безопасности с помощью видеоаналитики».*

14. **МТС**
Генеральный партнер конференции «Вызовы цифровой экономики и требования государства: найти баланс»

15. **Компания «Российские наукоемкие технологии» (РНТ)** — стенд; системный интегратор
Партнер деловой программы форума
Деловая программа:
- *«Безопасность против прогресса. Как найти золотую середину, или Особенности национальной безопасности»;*
- *«Сравнение технических решений реализации систем обнаружения вторжений»;*
- *«Современный кибертеррорист: кто он и как его победить?»*

16. **«Прософт-Биометрикс»** — биометрические системы информационной и технической безопасности
Коспонсор коференции «SecuFinance: защитные технологии банка будущего»
Деловая программа:
- *«Биометрическая идентификация для удобства клиента и предотвращения противоправных действий»*

17. **Прикладная радиофизика** — стенд; системы охраны периметра
Деловая программа:
- *«Прикладная радиофизика ТСО для периметров аэропортов на основе технологии «ВОРОН». Комплексные решения»;*
- *«Прикладная радиофизика ТСО для объектов ТЭК на основе технологии «ВОРОН». Комплексные решения».*

18. **ГК «Проинтех»** — стенд; программные комплексы поддержки принятия решений на базе биометрической видеоаналитики

19. **«Сфера»** — стенд; специализированное программное обеспечение
Деловая программа:
- *«От Безопасного города к Безопасному региону»*

20. **ГК ЦРТ** — стенд; системы биометрии, распознавания и синтеза речи
Деловая программа:
- *«Опыт построения систем видеоидентификации болельщиков на спортивных стадионах и ледовых аренах»;*
- *«Биометрия — новые возможности для финансового сектора».*

21. **«ЦеСИС НИКИРЭТ»** — комплексы инженерно-технических средств охраны
Деловая программа:
- *«Организация физической защиты периметра во время проведения спортивно-массовых мероприятий: инженерно-технические системы охраны объектов с массовым пребыванием людей»;*
- *«Применение противотаранной техники для обеспечения безопасности транспортных объектов. Проблемы и способы их решения».*

22. **Производственная фирма «ЭЛВИРА»** — стенд; нелинейная локация
Деловая программа:
- *«Инновационные отечественные нелинейные локаторы «ЛОРНЕТ»*

23. **«ЭЛВИС-ПЛЮС»** — стенд; системы безопасности и бизнес-мониторинга на основе технологий компьютерного зрения
Деловая программа:
- *«АПК «ЗАСТАВА-ТК» — универсальное рабочее место для корпоративных и государственных ИС»*

24. **AxxonSoft** — ПО для систем безопасности и видеонаблюдения
Коспонсор конференции «SecuRetail: комплексная безопасность торговых центров и ритейла»
Деловая программа:
- *«Интеллектуальное видео в ритейле. На службе оптимизации процессов и увеличения прибыли»*

25. **BEWARD** — стенд; разработчик и производитель IP-камер
Партнер форума
Деловая программа:
- *«Мировой опыт реализации проектов «Безопасный город»;*
- *«Системы видеонаблюдения как основа транспортной безопасности».*

26. **Facepass** — стенд; технологии распознавания лиц
Деловая программа:
- *«Обеспечение безопасного доступа в госорганизации, на предприятия и в банки с помощью ПАК «Система автоматического получения пропусков, билетов, гостевых карт и прохода с распознаванием лиц с минимальным участием персонала Facepass»*

27. **Fujitsu** — инфраструктурные решения
Деловая программа:
- *«Биометрия по венам ладони. Новые решения от производителя»*

28. **Huawei** — стенд; поставщик инфокоммуникационных решений
Партнер форума

29. **MobilityLab** — стенд; программные решения
Сопартнер конференции «Актуальные вопросы защиты информации»

30. **NEC NEVA** — стенд ROTOBO, сетевые коммутационные решения
Коспонсор конференции «SecuFinance: защитные технологии банка будущего»

31. **Японская ассоциация ROTOBO** — стенд; различные системы безопасности (защитное стекло от обледенения, решения по информационной безопасности и др.)
Деловая программа:
- *«Безопасность и перспективы развития индустрии дронов»*

32. **Tevian** — стенд; видеоаналитика и биометрия
Деловая программа:
- *«Распознавание лиц в ритейле»*

33. **Videointellect** — технологии видеоанализа
Партнер секции конференции «От Безопасного города к Безопасному региону»
Деловая программа:
- *«Actionrecognition как драйвер развития отрасли интеллектуального видеонаблюдения для обеспечения безопасности общественных мест»*

34. **VisionLabs** — стенд; технологии распознавания лиц
Деловая программа:
- *«Распознавание и анализ лиц для применения в ритейле»;*
- *«Распознавание и анализ лиц для применения в финансовой сфере».*

35. **Vocord** — стенд; системы безопасности на базе машинного зрения и интеллектуальных алгоритмов обработки видео

36. **Vzor** — стенд; системы биометрической идентификации человека

37. **Winkhaus** — стенд; системы контроля доступа
Деловая программа:
- *«Использование беспроводных систем контроля доступа в современном проектировании и строительстве»*

ПУСТО НЕ БЫВАЕТ

Количество экспонентов на ТБ Форуме в 2018 году приросло на четыре стенда по сравнению с 2017 годом и составило 56 стендов. Правительственная делегация сразу после открытия совершила официальный осмотр экспозиции, с остановками у 20 компаний (организаторы и сами компании не уточняют — входит ли это в стандартную стоимость пакета). Старт обходу дал стенд консорциума «Интегра-С» с уже привычными ГИС-решениями для контроля безопасности территорий, конечным пунктом стал стенд компании «Лорнет», поставляющей многофункциональные нелинейные локаторы для военных и спецслужб.

Неожиданно много компаний представили решения для видеоидентификации и видеоаналитики: Vzor, VisionLabs, Vocord, Tevian, Facepass, ЦРТ, NEC и даже широко не представленный на рынке бренд «Проинтех» (предлагал решение по распознаванию эмоций человека по жестам и мимике).

Своей фирменной товарной позицией — носимыми видеорегистраторами для силовиков — на выставку вышел «БайтЭрг». Небольшой стенд многократно усилила презентация директора по маркетингу Евгения Ерошина с ключевым тезисом «Видеонаблюдение — оружие справедливости!» Их старинный партнер по отрасли — компания Beward — сделала шаг к новым сегментам. Помимо камер подъездного видеонаблюдения ее инженеры продемонстрировали модели домофонов, потенциально актуальные для новых проектов «Ростелекома» по развитию так называемой «умной домофонии» (когда в устройство интегрированы сервисы, вплоть до снятия показаний с водо- и электросчетчиков).

И все же стенды — традиционно не главное на ТБ Форуме. Отработанный «Гротеком» еще на All-over-IP формат докладов «от первых лиц» завоевал популярность и тут. Некоторые стендисты прошлых лет — та же STT Group или лауреат премии ЗУБР 2017 года инновационный центр «Бирюч» — перешли от экспонирования продукции к залам конференций и кулуарным обменам визитками с представителями чиновничества.

КОД БЕЗОПАСНОСТИ: 969

XVII Международная конференция «Терроризм и безопасность на транспорте» стала одной из самых содержательных на ТБ Форуме. Не зря эксперт комитета Госдумы по транспорту депутат Александр Старовойтов представил ее как «самую масштабную и старейшую конференцию». Даром, что якорный спикер — замминистра транспорта Николай Захряпин — посетить конференцию не смог, хоть и был заявлен в программе. Состав президиума вполне компенсировал эту потерю: **Владимир Черток** (Ространснадзор, замглавы), **Александр Корниенко** (Минтранс, департамент транспортной безопасности), **Сергей Большаков** (Совет Федерации).

Павел Колесников, начальник центра технического регулирования и каталогизации ФКУ НПО «СТиС» МВД России, сообщил, что по состоянию на февраль 2018 выдано 24 сертификата, в работе находится 170 заявок. Все сертификаты выданы по так называемой 3-й схеме, на серийное производство. А это значит, что никто из транспортников еще не сертифицировал оборудование по 4-й схеме на объекте, как предполагает постановление правительства № 969.

Колесников честно предупредил коллег по отрасли, представителей объектов транспортной инфраструктуры: «Не рекомендую затягивать, орган по сертификации вправе принять решение об отзыве заявки, если заявитель долго не подписывает договор». Посыл был адресован тем руководителям объектов, кто уклоняется от уплаты штрафов, прикрываясь фразой «мы в процессе сертификации».

При этом Колесников для снижения стоимости сертификации предложил транспортному сообществу аккредитовать свои лаборатории, т. к. именно на это звено приходится наибольшая часть затрат (услуги самого центра обходятся не более чем в 20 тыс.

На данный момент для сертификации по части МВД России аккредитованы две испытательные лаборатории: ФГУП НИИР (четыре площадки) и Филиал ОАО «Объединенная ракетно-космическая корпорация» —«Научно-исследовательский институт космического приборостроения».

Из презентации Павла Колесникова об аккредитации испытательных лабораторий

рублей). Правда, подчеркнул, что методики испытаний — документы ограниченного доступа, предназначены только для аккредитованных лабораторий.

Другой спикер, **Алексей Васильев**, заместитель генерального директора ФГБУ «Центр МИР ИТ» (сертификация систем и средств связи), сообщил, что центр сотрудничает с такими аккредитованными лабораториями, как ФГОБУ «МТУСИ» (площадки в Москве, Нижнем Новгороде и Ростове-на-Дону), АНО «Сертификационный центр Связь-Сертификат», ЗАО «Испытательный центр «МирТелеТест». Но выдал только два сертификата, и оба — компании «Форт-Телеком». Хотя заявок поступает достаточно, большинство оформлено неверно. Вместо сертификатов «МИР ИТ» выдал к февралю 2018 года 125 уведомлений о недостатке документов.

ПО НАКАТАННЫМ РЕЛЬСАМ

На заседании подсекции «Применение инновационных технологий в области обеспечения транспортной безопасности» **Александр Зажигалкин**, начальник Центра инновационного развития (филиал ОАО «РЖД»), изложил ключевые потребности и ожидания своего ведомства в части систем безопасности.

Итак, РЖД интересуют:

- комплексные средства безопасности;
- решения, уже внедренные на транспорте;
- максимально современное оборудование;
- экономическая эффективность решений — при задаче оснастить 20 000 объектов заказчик заинтересован экономить бюджеты.

«Предложения без сертификатов по 969-му даже не рассматриваем», — расставил все точки над «i» Зажигалкин.

Спикер также сообщил, что РЖД планируют профинансировать пять инновационных стартап-проектов в 2018 году, 20-25 проектов в 2019 году и до 40 проектов в 2020 году.

Продемонстрирован на ТБ Форуме был и такой сегмент поставок в РЖД, как будущее строительство высокоскоростных магистралей (ВСМ).

О том, как устроена модель комплексного обеспечения безопасности на ВСМ, рассказал Сергей Ярыгин, директор Центра транспортной безопасности Самарского Государственного университета путей сообщения (СамГУПС).

На протяжении всей магистрали будет проходить специальная патрульно-эксплуатационная дорога, которая позволит спасательным отрядам быстро выдвигаться в зону ЧП, будет построено 5 типов КПП, т. к. для прохода через действующие вокзалы из одних зон транспортной безопасности в другие везде разные требования. Проблема в том, что нормы проектирования не предусматривают и не предусматривали раздел «транспортная безопасность». Хорошо, что пункт управления будет единым. Для обеспечения комплексной модели защиты ВСМ будет привлечено около 1000 сотрудников, 25,5 тыс. камер видеонаблюдения.

Консультируясь с производителями, эксперты университета пришли к выводу, что можно увеличить расстояние между камерами интеллектуального видеонаблюдения. При этом в рамках реализации проекта ВСМ Москва — Казань — Екатеринбург будет установлено более 12 000 камер (посты электрической централизации, вокзалы и искусственные сооружения) и не менее 25 000 камер на перегонах. Схема видеонаблюдения включает в себя тепловизоры и закрывает весь периметр, в том числе под платформами.

ФИГУРЫ ВЫСШЕГО ПИЛОТАЖА

Секцию по авиатранспорту модерировал **Дмитрий Ковалев**, начальник управления транспортной безопасности Росавиации. Он обозначил, какие моменты должны учитывать собственники объектов транспортной инфраструктуры (ОТИ).

Во-первых, это оценка рисков и план уязвимости, на всех объектах должно быть проведено категорирование и должен быть составлен план обеспечения безопасности. При внесении изменений в план необходима дополнительная оценка уязвимости.

Во-вторых, с 2018 года в паспортах безопасности ОТИ должны быть указаны данные по аттестации сил, аккредитации подразделений, сертификации по требованиям постановления № 969. Без соблюдения этих условий, пообещал Ковалев, оценку уязвимости не утвердят.

Также Ковалев не без гордости отметил, что для проведения аттестации в систему Росавиации сейчас аккредитовано 3 вуза. Кроме того, руководители ОТИ могут привлекать стороннюю аттестующую организацию — Росавиация «дает добро».

Отдельно Дмитрий Ковалев назвал стоп-факторы для аттестации сил обеспечения транспортной безопасности (ОТБ). Часто в уставе юрлиц-заявителей элементарно отсутствует вид деятельности «Транспортная безопасность» либо нет важнейшего документа — положения о подразделении ТБ. Иногда, если организация не может обеспечить какое-то требование и предусматривает так называемую эквивалентную меру, предлагает подмену реальной меры по обеспечению безопасности на ОТИ. Ковалев однозначно дал понять: борьба с «эквивалентами» будет жесткой, иначе временные меры станут правилом, хотя по правилам ТБ вообще нет понятия «эквивалентной меры». В год проведения ЧМ-2018 полумеры и вовсе недопустимы.

Ковалев закончил свое выступление призывом к подразделениям ОТБ не экономить на штате. «Запруды на входных группах, когда один сотрудник у интроскопа отвлекся от аппарата на проведение досмотра, а второй с металлодетектором бегает вокруг, то кладь рассматривать в интроскопе некому, и движение встает. Посадить нужно трех человек и не скупиться, — призвал Ковалев соблюдать пункт 106 приказа Минтранса № 104. — Вы никуда не денетесь, один раз вложитесь и все».

УЧИТЕСЬ ПЛАВАТЬ

Заместитель начальника управления транспортной безопасности Росморречфлота Валерий Капралов был однозначен: ничего практически не сделано.

«Требования транспортной безопасности в рамках постановления правительства № 678 выполнило не более 70-80 объектов транспортной инфраструктуры. Можно сказать, что достижения у нас по постановлению никакие», — сказал Капралов во время своей секции на транспортной конференции. И тут же выяснилось, что у речников и водников те же проблемы, что и у авиационных компаний: наибольшие затруднения связаны с привлечением и формированием подразделений ОТБ. «Система аттестации — сложнейший процесс, нам поручили ряд документов разработать самим, но Росморречфлот никогда не занимался разработкой документов, соответственно акты застопорились». В итоге ведомство справилось с задачей и разработало 9 нормативно-правовых актов. Так что теперь соблюдение требований по ОТБ — дело рук самих руководителей ОТИ на водном транспорте.

Программа форума

- Выездное заседание комитета Совета Федерации по обороне и безопасности
- Конференция «Обеспечение безопасности спортивных и массовых мероприятий» — Генеральный партнер темы: Группа «АСТЕРОС»
- Конференция «От Безопасного города к Безопасному региону» — Партнер: ВИДЕОИНТЕЛЛЕКТ
- Конференция «Вызовы цифровой экономики и требования государства: найти баланс» — Генеральный партнер: ПАО «МТС»
- Конференция «SecuRetail: комплексная безопасность торговых центров и ритейла» — Партнеры конференции: ITV|AxxonSoft, КРОК, СМ ТРЭЙД
- Конференция «Актуальные вопросы защиты информации» — Партнер: ГК «Конфидент» / Сопартнеры: Код безопасности / MobilityLab
- Конференция «Терроризм и безопасность на транспорте»
- Конференция «SecuFinance: защитные технологии банка будущего» — Коспонсоры: Прософт-Биометрикс, Инновационный центр безопасности, АО РНТ, VisionLabs, Fujitsu, NEC
- Конференция «Обеспечение комплексной безопасности и защищенности объектов промышленности, нефтегаза и энергетики»
- Конференция «Информационное моделирование в строительстве как основа безопасности инвестиций»
- «Круглый стол» «Инновационные технологии в области противопожарной защиты сложных и опасных промышленных объектов»
- «Круглый стол» «Безопасность и перспективы развития индустрии дронов»

ГЕРОИ ПОДЗЕМКИ

Андрей Кичигин, заместитель начальника ГУП «Московский метрополитен», начальник службы безопасности, демонстрировал работу подразделений ОТБ с помощью видеоролика на секции-практикуме «Актуальные вопросы обеспечения транспортной безопасности метрополитенов. Обеспечение комплексной безопасности транспортно-пересадочных узлов». Из его комментариев стало известно: в настоящее время метрополитены функционируют в 8 городах Российской Федерации. Суммарный суточный пассажиропоток может достигать 11 млн человек, что сопоставимо с населением средней европейской страны. А сами станции, с учетом неповторимых архитектурных особенностей, зачастую являются настоящим культурным достоянием и неотъемлемой частью большинства туристических маршрутов.

В качестве «оборотной стороны медали» Кичигин назвал замкнутость пространства, большую плотность пассажиров, возможность транспортного коллапса — и, увы, это то, что в первую очередь привлекает террористов.

«Мы регулярно сталкиваемся с трудновыполнимыми положениями отдельных руководящих документов. Например, идентификация выявленных при досмотре запрещенных предметов или веществ, составление многочисленных процедурных документов, а также огораживание контрольно-пропускных пунктов в целях исключения

возможности наблюдения за проведением досмотровых мероприятий. На наш взгляд, при большом пассажиропотоке и текущих архитектурных решениях такие требования попросту невыполнимы», — так звучит правда о безопасности метрополитенов в прямом изложении Кичигина. Технические сложности в обеспечении ТБ связаны с быстродействием интроскопов (на старых станциях они не всегда конвейерного типа) при сканировании багажа, т. к. напрямую влияют на численность и логику расстановки сил ОТБ.

Как начальник службы безопасности столичного метрополитена, Кичигин обратил внимание аудитории на такой эпизод ролика. Момент попытки проноса «тест-предмета» сотрудником ФСБ на станции «Ломоносовский проспект». Сотрудник сил ОТБ увидел подозрительный предмет в сумке, но вынужден был догонять «нарушителя», перехватывая его непосредственно у линейки турникетов. «Это связано с задержкой по времени при выводе на монитор содержимого 4-го сканируемого объекта, которая фактически позволила потенциальному террористу взять багаж и продолжить движение», — пояснил Кичигин и предложил производителям взять этот факт на заметку. Быстродействие оборудования — критически важное условие для метрополитена. Для работы в подземке необходимы также устройства для разделения пассажиропотока, портативные обнаружители паров взрывчатых веществ. Когда из зала заметили, что алгоритм действий на обнаружение таких веществ не разработан, Кичигин уверенно ответил: «Мы этим постоянно занимаемся, каждый инспектор знает, что ему нужно делать. Набираем постоянно молодых инспекторов, до 45 лет. Они более обучаемые».

Коллега Кичигина из Северной столицы — **Михаил Черников**, начальник отдела информационной безопасности ГУП «Петербургский метрополитен» — оценил как очень серьезные требования по постановлению правительства РФ № 495 к квалификации специалистов. «На объекте мы должны иметь трех досмотровиков, трех профайлеров, группу быстрого реагирования. Каждые 20 минут оператор у монитора интроскопа должен меняться», — отметил Черников и посоветовал готовить (обучать и аттестовывать) универсальных сотрудников, сразу по трем категориям.

На вопрос о ходе расследования теракта в питерской подземке Черников пояснил, что на данный момент расследование еще не закончено, ждут представления СК по устранению нарушений. «Могу сказать одно: в части выполнения всех требований обвинения должностным лицам не представлены, только отдельным сотрудникам на участке, где прошел нарушитель, за невыполнение обязанностей. В целом метрополитен все требования выполнил», — резюмировал Черников.

В ОЖИДАНИИ ПЕРЕМЕН

С каждой новой критикой пресловутый 16-ФЗ «О транспортной безопасности» становится все ближе к принятию в него поправок. Свой вклад в общее дело транспортной отрасли на ТБ Форуме внес **Евгений Ночкин**, начальник отдела транспортной безопасности департамента транспорта и развития дорожно-транспортной инфраструктуры Москвы. Он отметил, что закон формировался по образцу требований по авиационной безопасности и со временем противоречия реалий и требований закона стали критическими.

Например, в части закупочной деятельности — для муниципальных ОТИ на конкурс и процедуры уходит до полугода и даже больше, частные же структуры укладываются в три месяца, т. к. для них в законе прописаны только процедуры категорирования, проводить закупки по отдельной процедуре бизнес не обязан.

Похожая сумятица, по словам Ночкина, возникает и при реализации требований постановлений по транспортной безопасности. Так, на составление и реализацию планов обеспечения безопасности на объектах ОТИ вместо прописанных на бумаге двух лет на его реализацию фактическое время не превышает одного года.

Еще пример непродуманности требований — идентификация запрещенных веществ. В их перечень вошел вирус Эбола — для его выявления нужна лаборатория стоимостью в 1 млн евро, а требования предписывают наличие такого оборудования на каждой станции, посетовал Ночкин. Завершил свое выступление подчиненный Максима Ликсутова, вспомнив про Китай, где инспекторам скоро начнут выдавать очки со встроенным видеонаблюдением. Очки позволяют идентифицировать людей, а носимые видеорегистраторы, которые только-только входят в оборот российских силовиков, — нет.

ТЭК ПОД ЗАЩИТОЙ ГОСУДАРСТВА

Своеобразным трендом, который закрепился в начале 2018 года в направлении безопасности промышленных объектов и объектов ТЭК, стало усиление Росгвардии. К ведомству присоединен НИЦ «Охрана», а утвержденная «Концепция развития вневедомственной охраны на период 2018-2021 годов и далее до 2025 года» предусматривает выведение под контроль Рогвардии всей деятельности, содержащей в своем наименовании слово «охрана».

Уже сейчас ведомство проверяет антитеррористическую защищенность объектов ТЭК. О ходе этих проверок доложил **Игорь Фокин**, заместитель начальника Управления государственного контроля ГУЛРР И ГК Росгвардии. По его словам, в 2017 году ведомство проверило уровень безопасности на 2500 объектах ТЭК. В результате — 185 внеплановых проверок, к ответственности привлечены 62 руководителя объектов ТЭК, составлено 866 протоколов об административных правонарушениях. В целом результаты проверок свидетельствуют о позитивной тенденции в части приведения в состояние безопасности объектов ТЭК: из 1000 предписаний, выданных в 2017 году, по состоянию на 1 января 2018 года не исполнено лишь 79.

Игорь Фокин также сообщил, что в 2018 году Росгвардия планирует проверить соблюдение обязательных требований обеспечения безопасности на 2800 объектах ТЭК. При этом 1750 объектов будут проверяться впервые, а 1070 объектов — повторно.

Владимир Свинарев, советник президента ПАО «Транснефть», во время своего доклада на секции «Обеспечение комплексной безопасности и антитеррористической защищенности объектов ТЭК» заявил, что в компании настаивают на предоставлении ведомственной охране ПАО «Транснефть» полномочий по оформлению правонарушений, предусмотренных ст. 11.20.1 КоАП — «Нарушение запретов либо несоблюдение порядка выполнения работ в охранных зонах магистральных трубопроводов». В настоящее время полномочиями по оформлению протоколов по данным административным правонарушениям обладает Ростехнадзор. «Ведомственная охрана компании, специально созданная для защиты своих объектов, таких полномочий не имеет. Соответственно — правонарушения, многочисленные факты незаконной застройки охранных зон посредством возведения заборов, ограждений, заградительных конструкций, объектов капитального строительства жилого и нежилого назначения, которые нами обнаруживаются, остаются без должного внимания и правильной работы с ними», — пояснил Владимир Свинарев.

О СПОРТ, ТЫ — МИР!

Главной темой секции по безопасности массовых мероприятий стал Чемпионат мира по футболу FIFA-2018. **Александр Маслов**, заместитель начальника подразделения Центра ФСБ России, продемонстрировал макет персонифицированного паспорта болельщика (Fan-ID) с функцией идентификации лиц. Макет документа был представлен публике. Маслов отметил, что единый стандарт доступа на объекты, задействованные в массовых мероприятиях, с использованием персонифицированной карты зрителя и информационной системы контроля доступа сводят на нет влияние человеческого фактора со стороны контролеров и почти исключают вероятность несанкционированного допуска на объект лиц, не имеющих такого права. Надежность паспорта болельщика такова, что, получив Fan-ID и купив билеты на игру, иностранные зрители смогут въехать в Россию без визы. Упрощенный порядок начнет действовать за десять дней до первого матча и закончится через десять дней после финала.

Владимир Свинарев также отметил серьезность рисков незаконного вмешательства в деятельность магистральных трубопроводов компании. Это диктует необходимость усиления уголовной ответственности за преступления, предусмотренные ст. 215.3 УК РФ — «Приведение в негодность нефтепроводов, нефтепродуктопроводов и газопроводов».

«В связи с этим рассчитываем на поддержку рассматриваемого в Госдуме законопроекта, изменяющего диспозицию ст. 215.3 и устанавливающего криминализацию самовольного подключения к нефтепроводам, нефтепродуктопроводам и газопроводам либо приведения их в негодность, а также усиливающего уголовную ответственность за названные деяния», — подчеркнул Владимир Свинарев.

Также на секции были озвучены данные по использованию технических средств безопасности в рамках подготовки к ЧМ-2018. Так, в Москве на стадионе «Спартак» будет задействовано 130 камер в чаше стадиона и 60 городских камер на прилегающих территориях, на ЦСКА — 121 камера в чаше стадиона и порядка 60 городских камер. В «Лужниках» введено в эксплуатацию более 3 тыс. камер видеонаблюдения. Большинство камер на стадионах и прилегающих территориях уже интегрировано в государственную информационную систему «Единый центр хранения и обработки данных».

В Калининграде ожидают пятикратного роста количества видеокамер, число которых сейчас составляет 400 штук. На территории, прилегающей к стадиону «Калининград», установлено 300 камер видеонаблюдения. На четырех тренировочных площадках: стадионах «Пионер», «Локомотив», «Светлогорск» и спорткомплексе «Янтарный» — появится около 80 камер обзорного наблюдения. Еще 20 таких камер будет установлено в фан-зоне у Дома Советов.

На стадионе ФК «Краснодар» установлено около 1000 камер, которые передают всю информацию в Центр управления, в том числе в части распознавания лиц. Почти 400 камер видеонаблюдения установят в Нижнем Новгороде, и они будут включены в систему «Безопасный город». Сейчас в региональной системе работает 602 камеры.

В Саранске к ЧМ-2018 будет развернута интеллектуальная система видеонаблюдения, которая объединит 135 стационарных и 35 поворотных камер. В Ростове-на-Дону установили 106 дополнительных камер, а в Екатеринбурге появилось 1300 камер видеонаблюдения в дополнение к 378 действующим.

Помимо классических систем (видеонаблюдение, СКУД, пожарная сигнализация), на стадионах и объектах инфраструктуры будут использованы комплексы современных решений как отечественного, так и зарубежного производства — например, рентгенотелевизионные интроскопы для контроля ручной клади и личных вещей граждан, универсальные детекторы веществ, материалов и изделий повышенной опасности и т. д.

Юрий Исаев, начальник отдела Главного управления по обеспечению охраны общественного порядка МВД РФ, рассказал, как будет организована физическая охрана объектов. Так, к ЧМ-2018 на базе учебных заведений МВД создается Центр международного полицейского сотрудничества. В состав центра войдут полицейские офицеры всех государств, чьи национальные сборные будут выступать на чемпионате мира. По словам Исаева, создание такого центра происходит впервые в практике российских правоохранительных органов.

В целом охраной стадионов в период проведения ЧМ-2018 будут заниматься Росгвардия и другие правоохранительные структуры. Кроме того, обеспечивать безопасность будут около 15 400 сотрудников ЧОПов. Для работы на стадионах будет также привлечено более 16,5 контролеров-распорядителей, будет открыто 180 медицинских пунктов, задействовано 300 бригад «скорой помощи».

> Большинство камер на стадионах и прилегающих территориях уже интегрировано в государственную информационную систему «Единый центр хранения и обработки данных»

Также об опыте проведения массовых мероприятий доложили представители регионов, например Рыков Анатолий, первый заместитель главы города Сочи. О подготовке к ЧМ в Екатеринбурге рассказал Клюжин Евгений, председатель комитета органов администрации, муниципального образования «Город Екатеринбург».

Александр Мейтин, директор по безопасности российской футбольной премьер-лиги (РФПЛ), обратил в своем докладе внимание на детали, от них очень многое зависит. Даже такой незначительный факт, как отсутствие на предматчевом совещании руководителя оперативного штаба полиции, значительно усложняет взаимодействие. Его представитель, тоже присутствующий на совещании, как правило, не обладает правом принятия решений.

«В результате на самом матче ОМОН может, применяя специальные средства, производить жесткие задержания нарушителей порядка. Хотя их следовало проводить по окончанию матча, не на глазах у всего стадиона. Тем более что действия правонарушителей были зафиксированы камерами видеонаблюдения — и именно возможность такой ситуации обсуждалась на предматчевом совещании», — привел конкретный пример Мейтин.

ОТ «БЕЗОПАСНОГО ГОРОДА» К КСОБЖН

Участники конференции «От Безопасного города к Безопасному региону» были готовы поставить знак равенства между безопасным и умным городом. И модератор заседания **Александр Горбатько**, заместитель руководителя ДИТ Москвы, последовательно проводил эту мысль на примере столицы, где технологии «Умного города» уже служат безопасности. «Программа «Информационный город» предусматривает установку более 5 тыс. камер ежегодно. Процент покрытия жилого сектора средствами видеонаблюдения достигнет 90% к 2019 году», — рассказал чиновник.

Той же парадигмы придерживались и коммерческие спикеры от Huawey. Компания поставила «умные города» во главу своей маркетинговой стратегии и второй год подряд и при первой возможности делится своим опытом реализации подобных проектов в Кении, Гуаньчжоу, Сингапуре, Нью-Йорке и т. д. С недоверием собравшиеся отнеслись к сообщениям о 100%-ной раскрываемости убийств с помощью технологий компании, но за визиткой исправно подходили.

Однако все прогнозы по развитию умных и безопасных городов перекрыли в своих выступлениях представители МЧС и подведомственного министерству Всероссийского научно-исследовательского института по проблемам гражданской обороны и чрезвычайных ситуаций (ФГБУ ВНИИ ГОЧС).

Сначала **Ирина Олтян**, начальник научно-исследовательского центра ВНИИ ГОЧС, и ее

коллега **Елена Арефьева** вывели тему безопасности территорий на глобальный уровень. Не самым привычным в обсуждении безопасных городов стал отсыл к принципам Сендайской рамочной программы по снижению риска бедствий на 2015-2030 годы.

Как стало понятно из докладов представительниц ВНИИ ГОЧС, резолюцией Генеральной ассамблеи ООН определено, что начиная с 2018 года каждая страна должна осуществлять регулярную оценку выполнения 7 глобальных целевых задач Сендайской рамочной программы. В том числе Российская Федерация, которая поставила свою подпись под этой программой. В соответствии с принятой повесткой дня «Цель — устойчивое развитие», 11-я цель Сендайской рамочной программы касается устойчивого развития городов.

К 2020 году одна из задач — увеличить число городов и населенных пунктов, принявших и осуществляющих эффективные меры и комплексные планы и стратегии по снижению рисков бедствий.

На данный момент разработан и функционирует в Национальном центре управления в кризисных ситуациях (НЦУКС) программный комплекс динамического анализа природных, техногенных и биолого-социальных рисков на территории Российской Федерации.

Разработан, утвержден и введен в действие с 1 июня 2017 года национальный стандарт ГОСТ Р 22.10.02-2016 «Безопасность в чрезвычайных ситуациях. Менеджмент риска чрезвычайной ситуации. Допустимый риск чрезвычайных ситуаций».

В 2017 году разработан экспериментальный образец автоматизированной информационной системы стратегического прогнозирования в области гражданской обороны и защиты населения территорий от ЧС — так называемый АИС «Риск-Прогноз», основанный на новых качественных показателях риска, интегральных индексах риска, на основе анализа опасностей и угроз, потенциала противодействия и уязвимостей. В 2018 году запланировано создание опытного образца АИС.

> В 2018 году запланировано создание опытного образца АИС

В рамках реализации приоритетов Сендайской рамочной программы по МЧС России определена организация-координатор — это ВНИИ ГО ЧС. Подготовлен также межведомственный план реализации ее на национальном и местном уровне.

Развернута национальная кампания по повышению устойчивости городов и муниципальных образований в рамках глобальной стратегии ООН по повышению устойчивости городов к бедствиям «Мой город готовится».

Итогом выступлений Ирины Олтян и Елены Арефьевой стал принципиальный тезис: АПК «Безопасный город» — это реализация Сендайской рамочной программы по снижению риска бедствий на местном уровне. Что из этого следует, пояснил следующий докладчик — заместитель начальника ВНИИ ГОЧС **Сергей Качанов**.

Качанов, по сути, объявил новую парадигму в построении АПК «Безопасный город». В 2018 году МЧС завершит разработку и согласование новой Концепции комплексной системы обеспечения безопасности жизнедеятельности населения (КСОБЖН). Это глобальный проект, который вместит в себя и построение региональных систем — то есть, по сути, пояснил Качанов, над АПК БГ в России появится федеральный проект — КСОБЖН, с куратором в виде ВНИИ ГОЧС, который сформулирует правила устойчивого развития и безопасности для муниципальных территорий. Соответственно, можно предположить, что перечень технических средств и требований к ним для АПК «Безопасный город» производителям предстоит получать именно во ВНИИ ГОЧС.

Свежую струю в обсуждения внес **Николай Ильин**, начальник управления

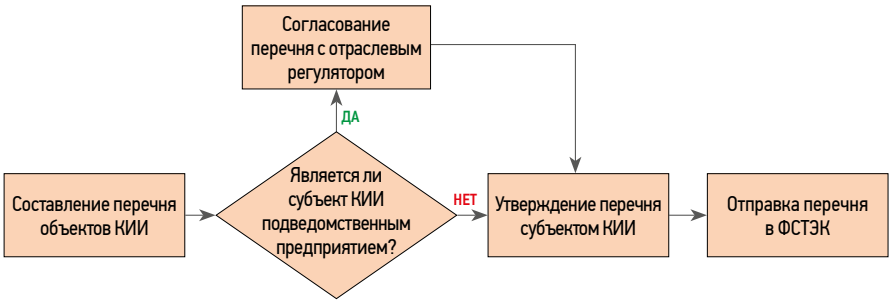
информационных систем Службы связи и информации ФСО России. Он рассказал о ходе строительства и задачах системы распределенных ситуационных центров (СЦ) в целях повышения эффективности работы губернаторов. СЦ должны быть использованы для решения самых разных задач — от обороны и безопасности до предотвращения этно-конфессиональных конфликтов, включая оценку экономической безопасности, мониторинг проблем социальной сферы и даже управление бюджетными ресурсами, реализацию приоритетных проектов и программ.

Однако, сразу оговорился Ильин, на данный момент создано 30 СЦ — в частности у всех полномочных представителей президента и в некоторых субъектах, например в Вологодской области, а также в Воронежской, Ивановской, Костромской областях, ХМАО.

24 центра создаются или модернизируются, 31 центр будет создаваться с нуля, в 8 субъектах решение о создании СЦ не принято (Адыгея, Дагестан, Карачаево-Черкесия, Кемеровская область, Камчатский край, Амурская область, Еврейская автономная область)

По данным Ильина, в России предстоит построить около 100 ситуационных центров. При озвучивании этой цифры представители регионов в зале заметно оживились. «Это же новый рынок, целое направление для развития», — переговаривались между собой заместители губернаторов и руководителей муниципальных образований.

Порядок согласования перечня объектов КИИ



ИНФОБЕЗОПАСНОСТЬ ОТ ФСТЭК. С КОММЕНТАРИЯМИ ЛУКАЦКОГО

Информационная безопасность (ИБ) традиционно собирает на ТБ Форуме аншлаги. Конференция Федеральной службы технического и экспортного контроля (ФСТЭК) «Актуальные вопросы защиты информации» в 2018 году выдалась особенно жаркой, т. к. вступивший в силу в январе 2018 года 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» вызвал много вопросов. Самый частый из них — как определить, к каким категориям критической информационной структуры (КИИ) относятся имеющиеся в организации информационные системы. Только во второй половине 2018 года планируется выпустить единую методичку ФСТЭК по мерам защиты, которая придет на смену существующей методичке по мерам защиты в ГИС. Поэтому как нельзя кстати были разъяснения новых требований, данные непосредственно представителями ФСТЭК.

Модератором конференции выступил начальник управления ФСТЭК России **Дмитрий Шевцов**. Вводится три категории значимых КИИ (наивысшая — первая), к четвертой категории можно отнести КИИ, не попавшие под критерии значимости, перечисленные в приложении к постановлению. Так, если нарушение функционирования сети связи затронет не всю территорию муниципального образования и без связи останется менее 50 тыс. человек, то по этому показателю КИИ не относится к значимым, если всю (или если без связи останутся от 50 тыс. до миллиона человек) — к третьей категории. Если территория, на которой возможно прекращение или нарушение функционирования сети связи, выходит за границы субъекта Федерации (или без связи останется более 5 млн человек) — то к первой категории значимости.

Категорирование объектов КИИ проводится с учетом их политической, экономической, социальной, экологической значимости и важности для обеспечения обороны страны. Оценка проводится по каждому критерию, а категория присваивается по высшему значению.

ФСТЭК проверяет правильность категорирования, при необходимости отправляет материалы субъекту КИИ на доработку и вносит данные в реестр значимых объектов КИИ. Пересмотр категории значимости производится не реже, чем раз в пять лет.

Чтобы понять, является ли организация субъектом КИИ, нужно посмотреть уставные

Правила категорирования объектов КИИ в РФ

Этапы категорирования объектов КИИ РФ

Основные этапы категорирования объектов КИИ РФ	Результат
Создание комиссии по категорированию	Приказ о создания комиссии
Анализ исходных данных для категорирования	Перечень объектов КИИ, подлежащих категорированию. Направляется в ФСТЭК в течение 5 дней после создания перечня
Категорирование объектов КИИ	Акт категорирования объекта КИИ
Направление сведений о категорировании в ФСТЭК РФ (в течение 10 дней после создания акта категорирования)	Внесение в реестр значимых объектов КИИ

31 вопрос, который собрал эксперт по информационной безопасности Алексей Лукацкий от участников рынка и на которые в рамках конференции «Актуальные вопросы защиты информации» на ТБ Форуме ответил заместитель начальника 2-го управления ФСТЭК России Шевцов Дмитрий Николаевич.

01 *Когда примут нормативные акты к 187-ФЗ?*

Из 4 приказов ФСТЭК приняты регулятором все; 3 из них находятся на регистрации в Минюсте. По остальным НПА вопрос, соответственно, надо задавать ФСБ и Минкомсвязи.

02 *Считает ли ФСТЭК деятельность ведомственных/корпоративных центров ГосСОПКИ лицензируемой по ТЗКИ? Речь про конкретный вид деятельности — мониторинг событий ИБ.*

Если речь идет об оказании услуг третьим лицам, то да, деятельность лицензируется.

03 *Если речь идет о группе промышленных предприятий, для которых функции SOC выполняет управляющая компания, то нужна ли этой УК лицензия ФСТЭК на мониторинг ИБ?*

Обязательно нужна.

04 *На сайте ФСТЭК прямо указано, что направление документов с ИОД осуществляется только при наличии лицензии на ГТ. При этом переписка по проверке значимых объектов с субъектом КИИ минимум ДСП. Как ФСТЭК собирается организовать проверку субъектов, не имеющих данную лицензию? Это требование о наличии лицензии ГТ обещали убрать с сайта еще в 17-м году, я задавал вопрос в рамках оформления лицензий.*

Ограничение на ГТ касается только документов; на распространение другой информации таких ограничений нет.

05 *На сайте ФСТЭК опубликована выписка из плана по разработке документов на 2018 год. В нем только положение о сертификации СЗИ. Никаких изменений в 17/21/31 приказ не планируется, никаких дополнительных документов по КИИ. ФСТЭК не видит актуальности в изменении?*

Изменения в 17/21/31 приказы будут во втором полугодии 2018 года. В выписке из плана далеко не все запланированные документы.

06 *Почему не хотят привести меры защиты к 17/21/31/ КИИ к сквозной нумерации и единым наименованиям?*

Все будет сделано во втором квартале 2018 года.

07 *Почему не учтен опыт совместного использования 17 и 21 приказа при разработке приказа по КИИ? Речь про п. 27 приказа 17. Зачем дополнительные сложности для оператора ГИС, которая стала значимым объектом КИИ? Будет ли проводиться корреляция требований между КИИ и 17-м приказом. Вопрос особенно интересно стоит для тех владельцев не-ГИС, кто недавно попал под 17-й приказ, но также и попадает под КИИ.*

ФСТЭК не видит проблем с одновременным выполнением приказов по КИИ и по ГИС — выбирать по максимальному из требований.

08 *Как выделять объекты КИИ, например, у банков?*

Субъект КИИ сам определяет свои объекты и проводит границы.

09 *В проекте постановления правительства по категорированию объектов КИИ указано, что перед категорированием нужно согласовывать со ФСТЭК и отраслевым регулятором перечень объектов КИИ, подлежащих категорированию. Как должен выглядеть этот процесс? Что делать, если у ФСТЭК и отраслевого регулятора разные точки зрения на перечень объектов, подлежащих категорированию?*

В финальном тексте ПП-127 согласование осталось только с отраслевым регулятором.

10 *Согласно проекту постановления правительства по категорированию объектов КИИ, категория определяется при создании или модернизации объекта КИИ. Что делать с действующими объектами КИИ, модернизация которых в ближайшее время не предусмотрена?*

Согласно ПП-127 категорирование осуществляется и для действующих объектов КИИ, перечень которых надо составить после вступления в силу ПП-127.

11 *Объекты водоснабжения и водоотведения по закону не являются объектами КИИ, все верно?*

Четкого ответа нет — надо смотреть на виды деятельности конкретного субъекта. Про пищевую промышленность вообще забыли спросить — там картина непонятная, в списке критических отраслей их в принципе нет.

12 *Получение телеметрии с подстанций (без телеуправления) попадает под действие КИИ?*

Да, так как на основе телеметрии могут приниматься управляющие воздействия и решения.

13 *Когда актуален 31-й приказ, а когда подзаконники по 187-ФЗ?*

Если объект значимый, то используется приказ ФСТЭК по КИИ. Если объект незначимый, то можно применять как 31-й приказ ФСТЭК, так и приказ по КИИ.

14 *В соответствии с какими методическими документами предполагается проведение моделирования угроз на КИИ?*

Работа над документами ведется. Пока руководствоваться Банком данных угроз и здравым смыслом.

15 *Требуется ли сертификация на соответствие АСУ ТП требованиям ФСТЭК? Если да, то кто ее проводит? Может быть, достаточно декларации?*
Сертификация не предусмотрена — только аттестация по требованиям безопасности или приемочные испытания АСУ ТП, включая и защитные меры.

16 *Если сертификация требуется, то что должно сертифицироваться: программно-технический комплекс для создания АСУ ТП или АСУ ТП конкретного объекта? Или и то и то?*
Не требуется.

17 *На какие АСУ ТП распространяются требования приказа ФСТЭК? Обязательны ли они к исполнению? Каким образом осуществляется контроль исполнения требований?*
31-й приказ не является обязательным, и контроль исполнения его требований не предусмотрен в отличие от приказа по КИИ.

18 *Обязан ли проектировщик предусматривать в проектах АСУ ТП мероприятия по приведению системы в соответствие с требованиями ФСТЭК, или это решение принимает заказчик?*
Это ответственность заказчика, но проектировщику неплохо бы напоминить заказчику о требованиях по ИБ, если последний о них забыл.

19 *Есть производственный цех, например прокатный стан. Согласно документации стан состоит из 3 АСУ ТП. При составлении перечня объектов КИИ возможно 3 АСУ ТП объединить в один объект КИИ? Что может выступать основой определения границ информационных систем?*
Субъект КИИ сам определяет границы объекта. В данном случае это может быть и один объект КИИ и три.

20 *Есть группа промышленных предприятий, которые будут отнесены к КИИ. Есть управляющая компания. Будет ли ее головной офис являться субъектом КИИ? Нужно ли этому головному офису вообще проходить категорирование?*
Нужно смотреть конкретную ситуацию, но вероятнее всего головной офис будет тоже отнесен к КИИ.

21 *У предприятия есть корпоративная ИС, в которую стекается вся информация о деятельности предприятия, начисляется зарплата, делается отчетность для налоговой и т. д. Эту систему надо включать в перечень объектов КИИ?*

Ответить, не видя конкретной ситуации, затруднительно.

22 *Что будет считаться гостайной, упомянутой в 187-ФЗ?*
Ждем поправок в указ президента № 1203, которые подготовлены и в скором времени будут утверждены.

23 *Когда будет разработан методический документ по мерам защиты на объектах КИИ?*
2-й квартал 2018 года. Будет единая методичка по всем приказам ФСТЭК (17/21/31/КИИ).

24 *Как поступать с объектами, чьи категории не выше третьей, но если атака будет одновременно сразу на несколько из них, то ущерб может наступить как у 2-й или даже 1-й категории?*
Как предписывает категория; в данном случае 3-я.

25 *Какова юридическая судьба документов по КСИИ? И что делать, если на промышленном предприятии в нормативных актах упоминается этот термин? Менять?*
Забудьте про них. Меняйте КСИИ на КИИ.

26 *ИС бухгалтерии субъекта КИИ тоже будет относиться к объектам КИИ?*
Надо смотреть конкретную ситуацию, но она точно должна рассматриваться в рамках категорирования, но, возможно, она будет незначимым объектом КИИ.

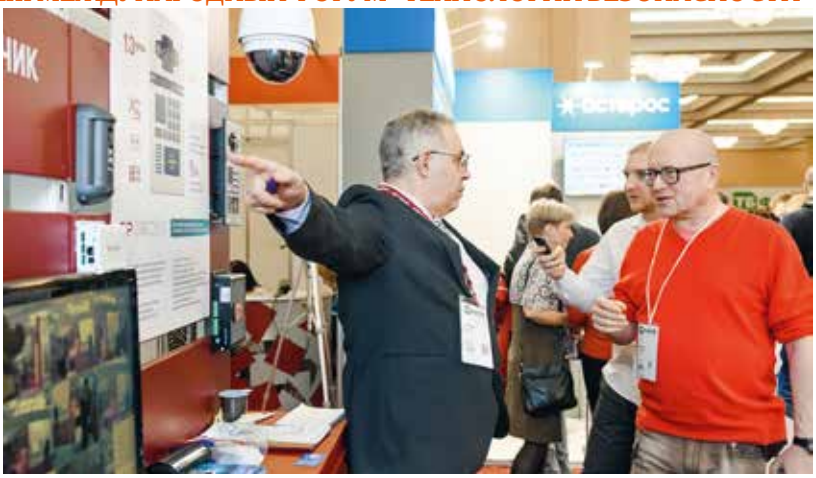
27 *Кто сертифицирует SIEM, используемые в SOCах, подключенных к ГосСОПКЕ, — ФСТЭК или ФСБ?*
Если речь идет об оказании услуг третьим лицам, то нужна лицензия ФСТЭК на мониторинг ИБ. Требования к лицензиатам доступны — требуется сертификация SIEM по требованиям ФСТЭК.

28 *Будет ли как-то описана/формализована процедура оценки соответствия средств защиты КИИ, отличная от сертификации (испытания и приемка), чтобы не иметь возможных претензий со стороны проверяющих?*
Все описано в 184-ФЗ о техническом регулировании и в соответствующих ГОСТах. Не надо бояться проверяющих — если они требуют не того, пишите/звоните во ФСТЭК.

29 *В последних сертификатах ФСТЭК отсутствует указание на соответствие требованиям по НДВ. Тем не менее приказ 17 требует применения средств, прошедших сертификацию на отсутствие НДВ для 1-го и 2-го классов. Каким образом владелец ИС в настоящее время может определить, проходило ли СЗИ такие испытания или нет?*
В новых РД ФСТЭК к средствам защиты уже прописано соответствие классов средств защиты и требований по НДВ. Если что-то непонятно, пишите вопросы во ФСТЭК — вам разъяснят про соответствие и выполнение требований по НДВ в конкретном продукте.

30 *В п.16.3 31-го приказа говорится о периодическом информировании и обучении персонала. Как подтвердить выполнение указанного пункта? Наличием плана обучения?*
Главное, чтобы люди были обучены, а как подтвердить это — вопрос десятый. Можно и планом обучения.

31 *Модель угроз должна разрабатываться для значимых объектов КИИ согласно приказам ФСТЭК. Значимый объект определяется по результатам категорирования, которое в свою очередь требует наличия модели угроз. Что первично?*
Как и в случае с ПДн (152-ФЗ и 21-й приказ), не надо путать перечень актуальных угроз и модель угроз. На этапе категорирования нужен только перечень актуальных угроз, а вот модель угроз как отдельный документ нужна уже на этапе реализации требований приказа ФСТЭК по КИИ.



документы, лицензии и другие разрешительные документы на виды деятельности и свериться с общероссийским классификатором видов экономической деятельности.

Исходные данные для категорирования объектов КИИ РФ

- Сведения об объекте КИИ
- Процессы (управленческие, технологические, производственные, финансово-экономические) в рамках выполнения функций субъекта КИИ
- Состав информации, обрабатываемой объектами КИИ, сервисы, предоставляемые объектами КИИ
- Декларация промышленной безопасности опасного производственного объекта, декларация безопасности гидротехнического сооружения, паспорт объекта ТЭК, на котором функционирует объект КИИ, если их разработка предусмотрена законодательством РФ
- Сведения о взаимодействии объекта КИИ с другими объектами КИИ
- Угрозы безопасности, а также данные о компьютерных инцидентах, произошедших на объектах КИИ данного типа

Если объект КИИ принадлежит одному субъекту, но в целях хозяйственной деятельности используется другим субъектом — в этом случае категорирование производит субъект, владелец КИИ, на основании данных, которые он получает от хозяйствующего субъекта.

Ответственность за правильное проведение категорирования КИИ не маленькая — получить по статье 274.1 УК РФ от 6 лет лишения свободы просто за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой в КИИ информации, либо до 10 лет, при наступлении тяжелых последствий из-за неправомерных воздействий на КИИ с 1 января наступившего года.

Категорирование, отметили представители регулятора, — только первый этап. Самое сложное — обеспечение безопасности КИИ. Причем чем выше значимость КИИ, тем требования будут жестче. И тут появляются новые возможности для аутсорсинга. Прежде всего аутсорсинга информационной безопасности, ведь большинству предприятий будет не по карману содержать специалистов по ИБ. Да и перекладывание ответственности на владельцев информационных инфраструктур будет способствовать росту использования облачных моделей. У дата-центра есть экспертиза, специалисты, программные и аппаратные средства обеспечения информационной безопасности. Провайдерам информационных инфраструктур легче обеспечить выполнение требований регуляторов.

Понимая это, организаторы конференции заняли вполне конструктивную позицию: вопросов много, но они решаемые. Главное — активно их задавать. Хозяйствующие субъекты получили прямое приглашение присылать свои вопросы на электронную почту ФСТЭК otd22@fstec.ru с пометкой «Вопросы по КИИ».

Эксперт по информационной безопасности Алексей Лукацкий так прокомментировал итоги конференции в своем блоге: «Я лично не вижу большой проблемы в составлении перечня объектов КИИ. Тут могут сильно помочь уже проведенные классификации ГИС, ИСПДн, АСУ ТП, КСИИ, ИСИОД, ИСОП и т. п.».

Области деятельности, в которых функционируют объекты КИИ

1. Здравоохранение
2. Наука
3. Транспорт
4. Связь
5. Банковская сфера и иные сферы финансового рынка
6. Топливно-энергетический комплекс
7. Атомная энергия
8. Оборонная промышленность
9. Ракетно-космическая промышленность
10 Горнодобывающая промышленность
11 Металлургическая промышленность
12 Химическая промышленность

РАССТАВИТЬ ПРИОРИТЕТЫ

Как можно видеть из данного, далеко не самого полного отчета, по итогам ТБ Форума 2018 года перед его организаторами стоит снять шляпу. Команда Андрея Мирошкина смогла удержать свою нишу, четко «разбанковав» тематики и спикеров между ТБ Форумом — который стал школой работы в государственных проектах, и форумом All-over-IP — где компании рынка безопасности обмениваются опытом в области технологий в формате нетворкинга. Кроме того, кажется, организаторы научились у своих экспонентов и работе в формате сервиса, обеспечивая постоянный, а не разовый контакт частных поставщиков с государственными клиентами — они, по сути, создали техподдержку бизнеса на проектном и GR-рынках.