SecurITy conference

# СИСТЕМЫ БЕЗОПАСНОСТИ КВОИ

## приоритизированный подход к созданию и совершенствованию

**Вячеслав Аксёнов**
ООО «ЮГИС групп»

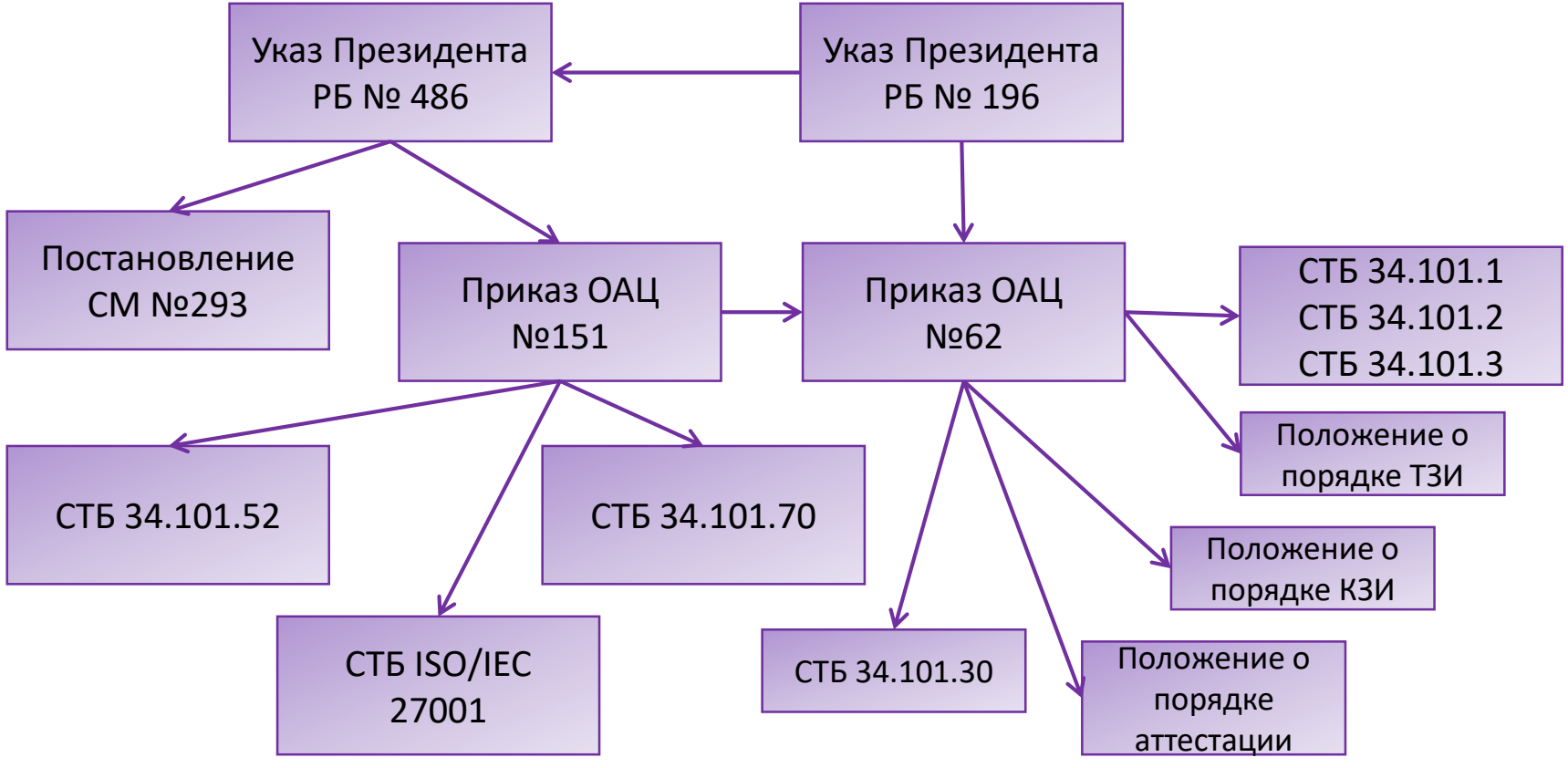
SecurITy conference

# В ДОКЛАДЕ:

- ✓ Требования по обеспечению безопасности КВОИ
- ✓ Структура СБ КВОИ
- ✓ Алгоритм и приоритизированный подход созданию и совершенствованию СБ КВОИ

!!! МНОГО дополнительных полезных материалов

# Требования


Указ Президента РБ № 486
Указ Президента РБ № 196
Постановление СМ №293
Приказ ОАЦ №151
Приказ ОАЦ №62
СТБ 34.101.1
СТБ 34.101.2
СТБ 34.101.3
Положение о порядке ТЗИ
СТБ 34.101.52
СТБ 34.101.70
Положение о порядке КЗИ
СТБ ISO/IEC 27001
СТБ 34.101.30
Положение о порядке аттестации

# Источники требований

ISO/IEC 27001:2013

NIST SP 800-82 R2 «Guide to Industrial Control Systems Security»

**Положение об обеспечении безопасности критически важных объектов информатизации,**
утвержденное приказом ОАЦ от 12.10.2018 № 151

NIST «Framework for Improving Critical Infrastructure Cybersecurity»

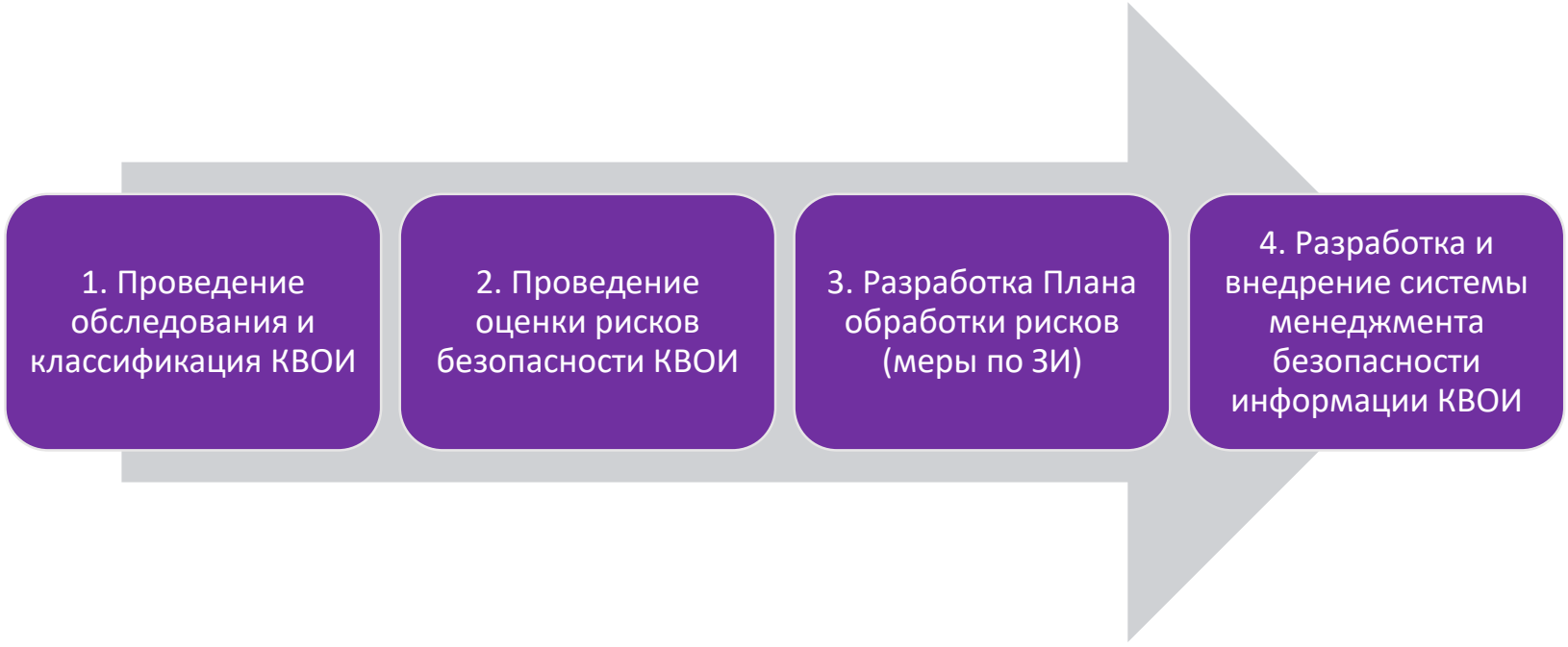
ENISA Publications

# Взаимосвязанность требований

| Приказ ОАЦ 151 | ISO/IEC 27001 | ISO/IEC 27002 | ISO/IEC 31000 | СТБ 34.101.70 | Приказ ОАЦ 62 |
|---|---|---|---|---|---|
| 7.5. определение физических и логических границ области применения системы безопасности | 4.3 | 8.1.1 | 4.3.1, 5.3 | | 7 |
| 7.6. инвентаризация (выявление и учет), а также определение степени важности (исходя из конфиденциальности, целостности и доступности) активов КВОИ | 6.1.2 | 8.1.1 | 5.4.2 | 5.1 | 7, П1_7.1, |
| 7.7. определение работников, ответственных за использование активов КВОИ | 5.3, 7.1, 7.2 | 6.1.1, 6.1.2 | 4.3.3, 4.3.5 | 5.1 | П1_3.5, П1_4.9 |
| 7.8. определение угроз безопасности КВОИ | 6.1.2 | 8.1.2 | 5.4.2 | 5.2 | 7 |

# Система безопасности

# Приоритизированный подход



# Приоритизированный подход

| | ОАЦ №151 | NIST «Framework for Improving Critical Infrastructure Cybersecurity» |
|---|---|---|
| Идентификация | п.5-7 | Управление Активами (Asset Management)<br>Бизнес Среда (Business Environment)<br>Руководство (Governance)<br>Оценка Риска (Risk Assessment)<br>Стратегия Управления Риском (Risk Management Strategy)<br>Управление Риском Логистической Цепочки (Supply Chain Risk Management) |
| Защита | п.9 | Управление Доступом (Access Control)<br>Повышение Осведомленности и Обучение (Awareness and Training)<br>Защита Данных (Data Security)<br>Процессы и Процедуры Защиты Информации (Information Protection Processes and Procedures)<br>Техподдержка (Maintenance)<br>Технология Защиты (Protective Technology) |
| Обнаружение | п.10-11 | Аномалии и События (Anomalies and Events)<br>Непрерывный Мониторинг Безопасности (Security Continuous Monitoring)<br>Процессы Обнаружения (Detection Processes) |
| Реагирование | Эксплуатация КВОИ | Планирование Реагирования (Response Planning)<br>Коммуникация (Communications)<br>Анализ (Analysis)<br>Подавление (Mitigation)<br>Улучшение (Improvements) |
| Восстановление | | Планирование Восстановления (Recovery Planning)<br>Улучшение (Improvements)<br>Коммуникации (Communications) |

# Результаты

| | | |
|---|---|---|
| Отчет по результатам проведении обследования КВОИ (Gap-анализ) | Акт классификации КВОИ | Методика оценки рисков безопасности КВОИ |
| Отчет по результатам оценки рисков безопасности КВОИ | План обработки рисков безопасности КВОИ | Политика информационной безопасности |

Комплект локальных нормативных правовых актов, регламентирующий вопросы обеспечения безопасного функционирования КВОИ (положения, регламенты, инструкции)

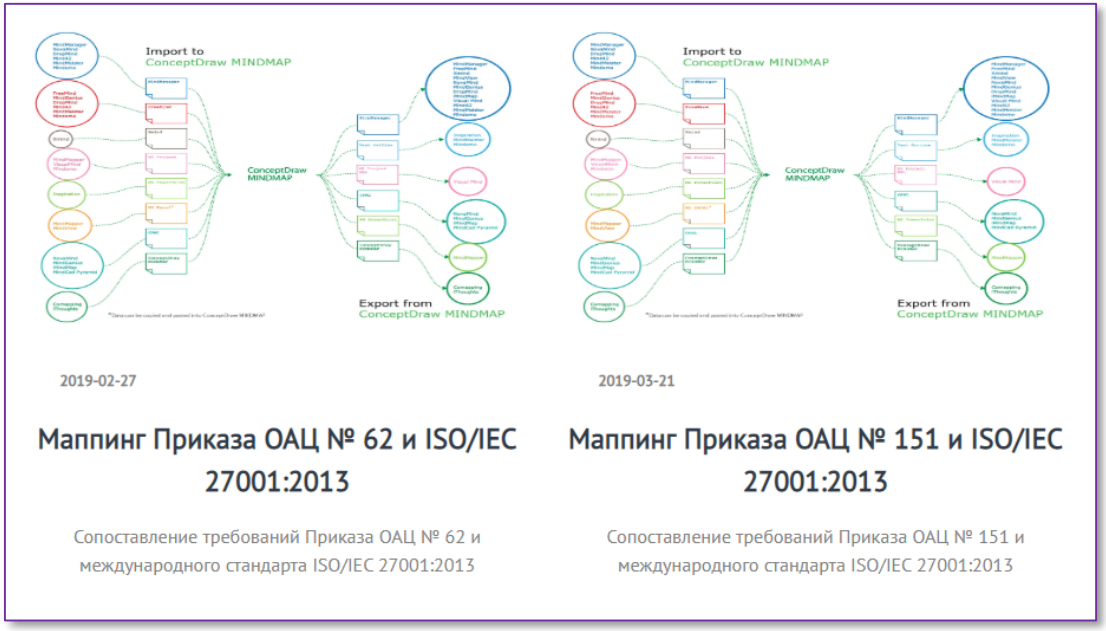
Отчет по результатам проведения оценки соответствия КВОИ требованиям приказа ОАЦ № 151 от 12.08.2018 г. и СТБ ISO/IEC 27001-2016

# Готовимся к проверке

| Требования приказа ОАЦ 151 | ЛНПА | СрЗИ / КЗИ, Автоматизация | Контроль |
|---|---|---|---|
| п.9: используются средства защиты информации от вредоносного программного обеспечения | Положение об обеспечении АВЗ | Средство АВЗ «XXX» | Отчет по результатам вн. аудита ИБ |
| п.9: распределены и согласованы обязанности работников и их ответственность по вопросам обеспечения безопасности КВОИ | Политика ИБ | n/a | Отчет по результатам вн. аудита ИБ |
| п.7.12: оценка рисков безопасности КВОИ | Отчет по оценке рисков | Система управления рисками «YYY» | n/a |

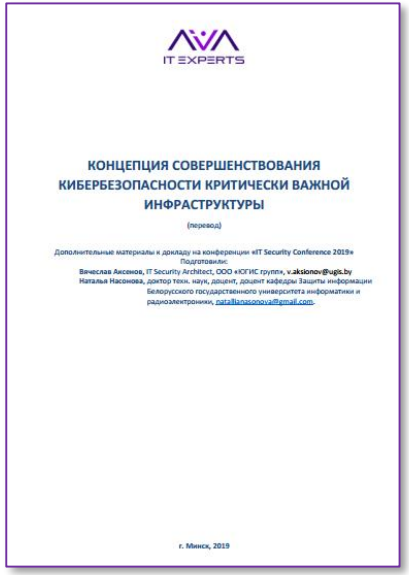
Secur IT y conference

# Маппинг Приказов ОАЦ 62 / 151 и ISO/IEC 27001




goo.gl/xx3ubF

NIST «Framework for Improving Critical Infrastructure Cybersecurity» (перевод на русский)



КОНЦЕПЦИЯ СОВЕРШЕНСТВОВАНИЯ КИБЕРБЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНОЙ ИНФРАСТРУКТУРЫ

(перевод)

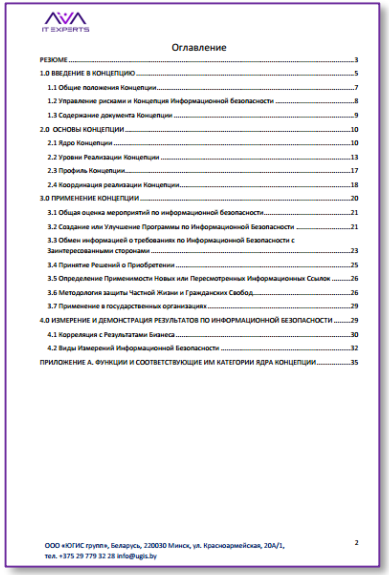
Дополнительные материалы к докладу на конференции «IT Security Conference 2019»

Подготовили:

Вячеслав Аксенов, IT Security Architect, ООО «ЮГИС групп», v.aksionov@ugis.by

Наталья Насонова, доктор техн. наук, доцент, доцент кафедры Защиты информации Белорусского государственного университета информатики и радиоэлектроники, natalliansonova@gmail.com.

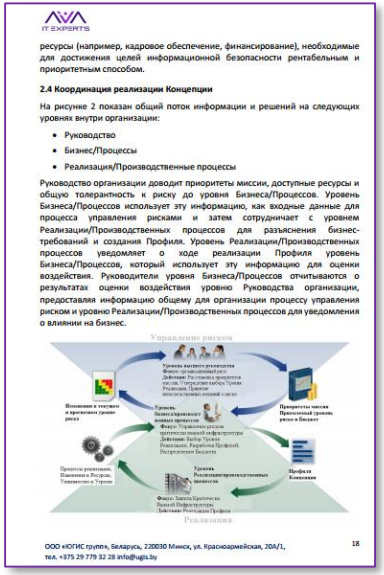
г. Минск, 2019



Оглавление



ООО «ЮГИС групп», Беларусь, 220030 Минск, ул. Красноармейская, 20А/1, тел. +375 29 779 32 28 info@ugis.by 2



ресурсы (например, кадровое обеспечение, финансирование), необходимые для достижения целей информационной безопасности рентабельным и приоритетным способом.

**2.4 Координация реализации Концепции**

На рисунке 2 показан общий поток информации и решений на следующих уровнях внутри организации:

- Руководство
- Бизнес/Процессы
- Реализация/Производственные процессы

Руководство организации доводит приоритеты миссии, доступные ресурсы и общую толерантность к риску до уровня Бизнеса/Процессов. Уровень Бизнеса/Процессов использует эту информацию, как входные данные для процесса управления рисками и затем сотрудничает с уровнем Реализации/Производственных процессов для разъяснения бизнес-требований и создания Профиля. Уровень Реализации/Производственных процессов уведомляет о ходе реализации Профиля уровень Бизнеса/Процессов, который использует эту информацию для оценки воздействия. Руководители уровня Бизнеса/Процессов отчитываются о результатах оценки воздействия уровню Руководства организации, предоставляя информацию общему для организации процессу управления риском и уровню Реализации/Производственных процессов для уведомления о влиянии на бизнес.




ООО «ЮГИС групп», Беларусь, 220030 Минск, ул. Красноармейская, 20А/1, тел. +375 29 779 32 28 info@ugis.by 18

goo.gl/2qBs44

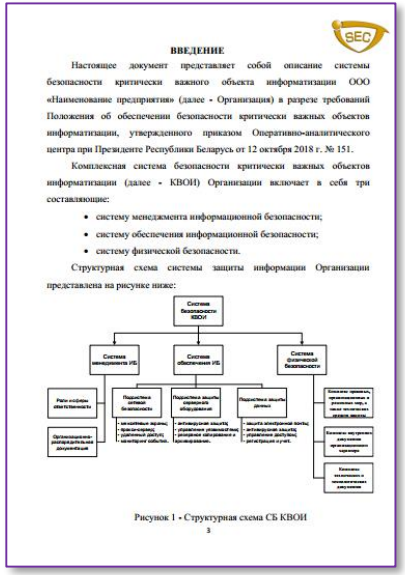
Security conference

# «Система безопасности КВОИ. Описание» (шаблон)

КРИТИЧЕСКИ ВАЖНЫЙ ОБЪЕКТ
ИНФОРМАТИЗАЦИИ.
СИСТЕМА БЕЗОПАСНОСТИ

Разработал:
Должность _____ И.О. Фамилия
(подпись) ( дата)

2019



ВВЕДЕНИЕ

Настоящее документ представляет собой описание системы безопасности критически важного объекта информатизации ООО «Наименование предприятия» (далее - Организация) в разрезе требований Положения об обеспечении безопасности критически важных объектов информатизации, утвержденного приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 12 октября 2018 г. № 151.

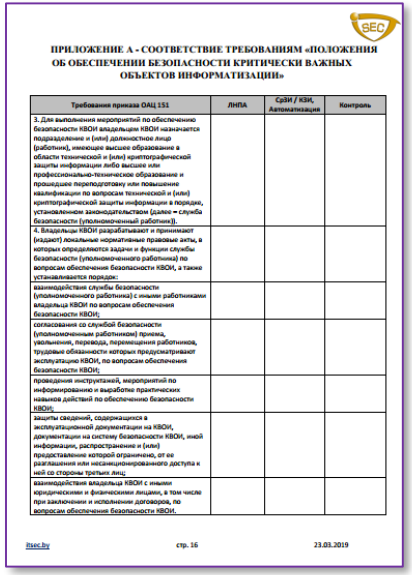
Комплексная система безопасности критически важных объектов информатизации (далее - КВОИ) Организации включает в себя три составляющие:

- систему менеджмента информационной безопасности;
- систему обеспечения информационной безопасности;
- систему физической безопасности.

Структурная схема системы защиты информации Организации представлена на рисунке ниже:

Рисунок 1 - Структурная схема СБ КВОИ

3



ПРИЛОЖЕНИЕ А - СООТВЕТСТВИЕ ТРЕБОВАНИЯМ «ПОЛОЖЕНИЯ ОБ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ»

| Требования приказа ОАЦ 151 | ЛНПА | СрЗИ / КЗИ, Автоматизация | Контроль |
|---|---|---|---|
| 3. Для выполнения мероприятий по обеспечению безопасности КВОИ владельцем КВОИ назначается подразделение и (или) должностное лицо (работник), имеющее высшее образование в области технической и (или) криптографической защиты информации либо высшее или профессионально-техническое образование и прошедшее переподготовку или повышение квалификации по вопросам технической и (или) криптографической защиты информации в порядке, установленном законодательством (далее – служба безопасности (уполномоченный работник)). | | | |
| 4. Владельцы КВОИ разрабатывают и принимают (издают) локальные нормативные правовые акты, в которых определяются задачи и функции службы безопасности (уполномоченного работника) по вопросам обеспечения безопасности КВОИ, а также устанавливается порядок: | | | |
| взаимодействия службы безопасности (уполномоченного работника) с иными работниками владельца КВОИ по вопросам обеспечения безопасности КВОИ; | | | |
| согласования со службой безопасности (уполномоченным работником) приема, увольнения, перевода, перемещения работников, трудовые обязанности которых предусматривают эксплуатацию КВОИ, по вопросам обеспечения безопасности КВОИ; | | | |
| проведения инструктажей, мероприятий по информированию и выработке практических навыков действий по обеспечению безопасности КВОИ; | | | |
| защиты сведений, содержащихся в эксплуатационной документации на КВОИ, документации на систему безопасности КВОИ, иной информации, распространение и (или) предоставление которой ограничено, от ее разглашения или несанкционированного доступа к ней со стороны третьих лиц; | | | |
| взаимодействия владельца КВОИ с иными юридическими и физическими лицами, в том числе при заключении и исполнении договоров, по вопросам обеспечения безопасности КВОИ. | | | |

ihec.by стр. 16 23.03.2019

goo.gl/6HNrHb

SecurITy conference

# СПАСИБО ЗА ВНИМАНИЕ!

**Вячеслав Аксёнов**
ООО «ЮГИС групп»
v.aksionov@ugis.by