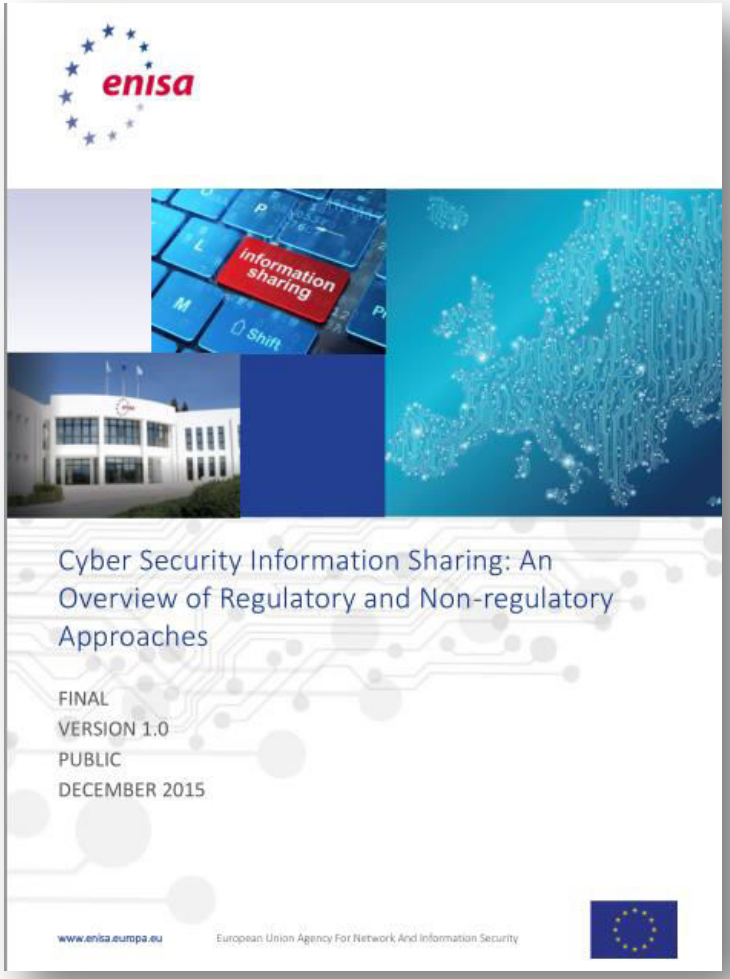
РИФ+КИБ 2016

Обмен информацией в области безопасности. Подходы к регулированию. Опыт Европы

Ассоциация
«Открытая Сеть»

13.04.2016

Отчет ENISA



Отчет об исследовании **«Обмен информацией в области кибер-безопасности. Обзор регуляторных и нерегуляторных подходов»**;
Джо Де Манк,
Др. Сильвиа Портези;
ENISA, Deloitte (Бельгия);
декабрь 2015

Роль и место ENISA в контексте Евро CSS

Обмен информацией, выгоды и риски

Общий обзор регуляторных подходов и инициатив

TRADITIONAL REGULATION	ALTERNATIVE FORMS OF REGULATION	OTHER APPROACHES
Command-and-control legislation, legally binding rules: coercive rules are implemented and organisations need to comply with these legally binding rules. • e.g. Electronic identification and trust services (eIDAS) Regulation • e.g. Telecom laws in Belgium, Lithuania, Spain • e.g. Electronic Communication Act in Slovenia • e.g. Information Society Code in Finland • e.g. Security measures acts in Estonia, Germany	**Co-regulation:** the regulatory body gives power and entrusts market stakeholders to achieve a policy objective. • e.g. Information Sharing and Analysis Centres (ISACs) in the Netherlands • e.g. Information Exchanges (IEs) in the United Kingdom • e.g. UP KRITIS in Germany • e.g. Austrian Trust Circle (ATC in Austria • e.g. Threat indicators sharing platform for private sector (MISP) in Luxembourg • e.g. Forum for information sharing (FIDI) in Sweden **Self-regulation:** market stakeholders agree and create on a voluntary basis rules to regulate their actions. • e.g. Industrial Cybersecurity Centre (CCI) in Spain • e.g. n6 Network Security Incident Exchange and ABUSE Forum in Poland • *Club des directeurs de sécurité des entreprises* in France • *Associazione italiana esperti in infrastructure critiche* (AIIC) in Italy • e.g. Bulgarian Association of Information Technologies (BAIT) e.g. Information Technology and Information Systems Security Experts Group (DEG) in Latvia	**Information and education:** enhance the knowledge of the community on a certain topic to change its behaviour. • e.g. workgroups held by Czech CSIRT in Czech Republic • e.g. Belgian Network and Information Security (BELNIS) in Belgium • e.g. (ISC)² Ireland Chapter in Ireland • e.g. Cyber Security Research Center from Romania (CCSIR) in Romania

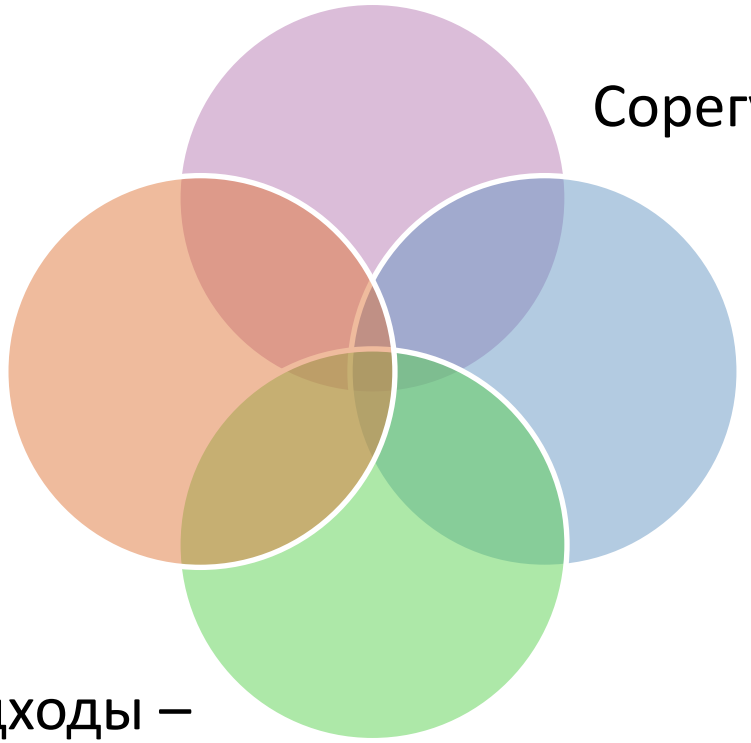
Кибериниденты в контексте Евро CSS

CATEGORIES OF CYBER INCIDENTS	AREAS OF CYBER SECURITY
Incidents having a serious impact on business continuity of **networks and services**.	✓ Critical Infrastructure Protection (CIP)
	✓ Critical Information Infrastructure Protection (CIIP)
Incidents relating to a **crime** that would require the preservation of evidence, identification of the perpetrators and ultimately assurance that they are prosecuted.	✓ Cyber crime
	✓ Cyber safety
Incidents compromising **personal data**.	✓ Privacy breaches
	✓ Cyber crime (identity theft, fraud, ransomware…)
	✓ Cyber safety

Критические сектора в контексте Евро CSS

SECTOR	RATIONALE FOR INCLUSION IN SCOPE OF THIS STUDY BASED ON THE IMPACT ASSESSMENT
Energy	Generation, transmission and distribution of energy are highly dependent on secure network and information systems. Major gas and electricity companies for example, suffer increased amounts of cyber attacks motivated by commercial and criminal intent.
Transportation	Key transport infrastructure such as airports, ports, railways, traffic management systems and logistics suffer increased amounts of cyber attacks motivated by commercial and criminal intent.
Health	Hospitals and clinics are becoming more reliant on sophisticated ICT systems which need to be secure in order to ensure continuity of service and avoid fatal disruptions.
Finance and banking	Banks are the backbone of our financial system. They are common targets of fraudsters. The stock exchange, insurance, retail and investment banking for example, are increasingly adopting networks and information systems and Internet based commerce systems.
Internet services	It is important to ensure the security of Internet companies which provide key inputs enabling important economic and societal processes. This is essential to preserve trust in the digital ecosystem.
Public administration	E-Government and e-participation are increasing with citizen demand for timely and cost-effective services and so are the NIS risks for state and local administrations. The risk for public online services to be hindered by NIS problems exist at all levels.

Подходы к регулированию



Сорегулирование

Традиционное регулирование

Само-регулирование

Другие подходы – информирование, обучение и т.п.

Традиционное регулирование

Регулирование:

соотносится с правилами или порядком, предписанным для менеджмента организаций и правительств, а также регулирующими принципами и предписаниями.

Как правило, предписано вышестоящим руководителем или компетентным органом субъектам, находящимся в его ведении или под его контролем.

(InterActive Terminology for Europe, 2014)

Сорегулирование

Сорегулирование:

механизм, посредством которого законодатель возлагает достижение целей, предусмотренных законодательством или другими документами политик, на субъектов, признанных в соответствующей сфере деятельности.

К таким субъектам относятся коммерческие и некоммерческие организации, их объединения, ассоциации и т.п.

(Европейская Комиссия, 2015)

Саморегулирование

Саморегулирование:

соотносится с группами хозяйствующих субъектов определенного сектора, отрасли или сферы профессиональной деятельности, добровольно разрабатывающих и применяющих стандарты, правила и кодексы участия в группе и ведения деятельности, которые регулируют или направляют их деятельность

(ОЭСР, н/д)

Вызовы традиционного регулирования

1	Различия требований в странах-членах, а также в рамках одной страны на региональном или отраслевом уровне
2	Коллизии с национальным законодательством по локализации обработки данных, об ограничении сбора и хранения данных, об обеспечении секретности и конфиденциальности данных
3	Практики заключения договоров с поставщиками и потребителями, корпоративных и административных соглашений, включающих положения о неразглашении

Вызовы сорегулирования

1	Недостаточность взаимного доверия, мотивов и механизмов побуждения к участию в инициативе и к обмену информацией
2	Баланс между размером сообщества, рисками утеря контроля над информацией и невключения в сообщества критически важного участника
3	Баланс ценности участия в сообществе и получения информации и рисков огласки, потерь и санкций

Вызовы саморегулирования

1	Добровольность присоединения к инициативе и следования ее правилам
2	Недостаточность взаимного доверия, опасения ущерба
3	Коллизии с традиционным регулированием в части ограничения оборота информации или ее обязательного раскрытия
4	Неопределенность предписаний механизма светофора
5	Несогласованность с предписаниями государственных систем классификации информации ограниченного доступа

Вызовы других подходов - информирования, обучения

1	Необходимость доверия и авторитета координатора инициативы и источников
2	Размеры сообщества и взаимное доверие участников
3	Соответствие законодательству и документам средне- и долгосрочных политик
4	Сложность оценки результативности и эффективности изменений
5	Длительность процесса изменений

7 рецептов

1	Создавайте неформальные сообщества
2	Вовлекайте участников по горизонтальным и вертикальным связям основного бизнеса
3	Заведите на своей инфраструктуре список рассылки, блог, wiki
4	Проводите очные встречи участников сообщества
5	Просите содействия, привлекайте к участию вендоров, интеграторов и поставщиков сервисов
6	Взаимодействуйте с инициативами в других секторах, отраслях и регионах
7	Оформляйте, «легализуйте» сообщества

РИФ+КИБ 2016

За безопасность вместе!

Георгий Грицай
info@theopennet.ru

Ассоциация
«Открытая Сеть»

13.04.2016