Контентная безопасность : ситуация в Европе и мире

Неделя Безопасного Рунета \ CyberSecurityForum - 2018,
6 февраля 2018 г.

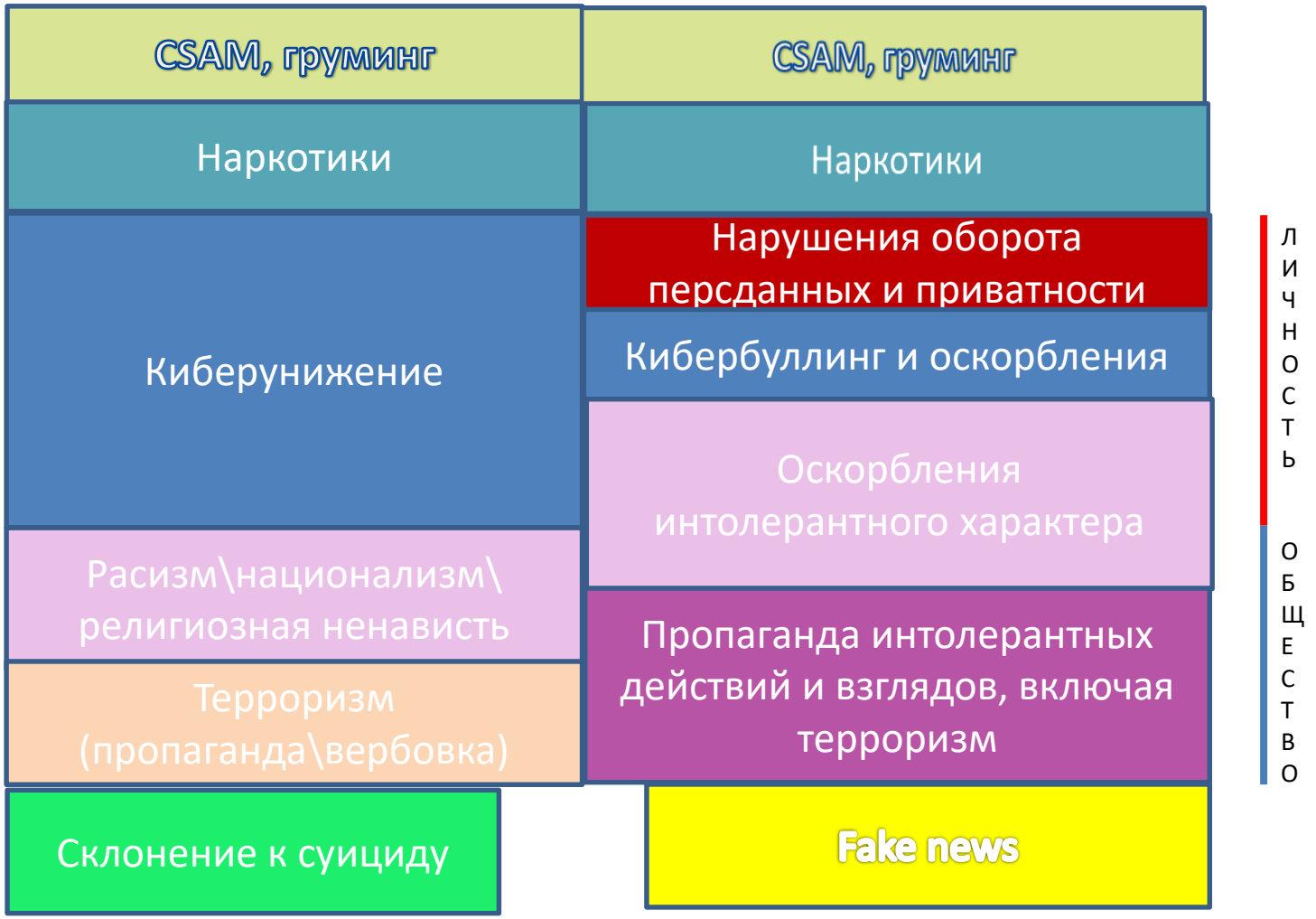
Контентные и околоконтентные угрозы: ситуация-2017

Принципиально список контентных угроз не изменился. Новые угрозы – как правило, вариации существующих.

Однако восприятие этих угроз различно.

Каждому континенту свойственны собственные приоритеты угроз.

Россия и Европа: соотнесение контентных угроз



Статистически это выглядит так:

Сцены сексуальной эксплуатации детей:

38 676 URL за последний отчетный год внесено в БД INHOPE – Interpol

Всего в БД – 9 357 240 URL

Тренд 2017 года для России – возврат к формату-2009: возвращение сайтов с отдельными URL, соцсети ушли на третье место (второе – торренты)

Киберунижение – «угроза №1», только по «Линиям помощи» свыше 356 000 обращений (ЕС+Россия, не считая «Горячих линий» и статистики индустрии)

Наркотики – рост числа сообщений с 2014 года, сайты и форумы, иностранная юрисдикция, маскировка под стероиды

Экстремизм – рост в Европе (по категории hate speech), в России ситуация не меняется (главный тренд – политизация обращений)

Почему такая разница в трендах?

Разная проработанность механизмов борьбы с различными угрозами

	CSAM	Экстремизм	Киберунижение
Информационно-просветительская работа	Да, сниженная	Да, средняя	Да, активная
Прием сообщений о противоправном контенте	100% ГЛ INHOPE	50% ГЛ INHOPE	30% ГЛ INHOPE
Механизм трансграничной обработки и передачи сообщений	Да	Нет	Нет
Вовлеченность правоохранителей	Сильная (включая Интерпол)	Слабая, на национальном уровне	Нет
Консультационно-реабилитационная работа	Да	Нет	Да
Вовлеченность Интернет-индустрии	Большая	Средняя	Средняя

Почему нет системы борьбы с киберунижением, аналогичной CSAM?

- Недостаток знаний в области прав человека, путаница между защитой приватности и гарантией свободы слова;
- Сильнейшее недоверие к государственным и надгосударственным органам, боязнь использования прецедента для введения цензуры;
- Заблуждения относительно необходимости санкций, следующие из текущей европейской концепции «прав детей».

А также:

- Неготовность к тщательному анализу контента, т.к., в отличие от CSAM, контент текстовый и допускает субъективные интерпретации;
- Боязнь вовлечения правоохранителей (за исключением англосаксонских стран), преувеличенная вера в перекос воспитательного процесса;
- Неготовность организаций, наработавших опыт в сфере борьбы с CSAM, брать на себя дополнительную тематику.

Итог:

- Однобокость системы с перекосом в информационно-просветительскую работу без эффективных профилактических и реактивных механизмов;
- Единственный эффективный лоббист системы борьбы с киберунижением – Еврокомиссия.

Что меняется?

Новеллы в основном связаны с киберунижением. При разнесенности по времени к 2017 году они приобрели некую системность:

- 2016 – Code of Conduct Against Hate Speech по инициативе Еврокомиссии: документ саморегулирования, однако устанавливает конкретные практические обязательства для подписантов и мониторинг Еврокомиссии за их исполнением;
- Май 2018 – вступление в силу GDPR: абсолютизация понятия «персональные данные» и распространение законодательства о персданных на любое прямое или косвенное упоминание личности, включая право требования удаления данных;
- Приоритизация понятия «приватность» над понятием «общественная значимость» для всех, кроме публичных политиков и чиновников, в глазах еврорегулятора;
- Инициирование создания системы трансграничного обмена информацией по случаям hate speech по образцу борьбы с CSAM: автоматизированный реестр, система уведомления ГЛ об инцидентах, взаимодействие с индустрией и правоохранителями. На основе действующих ГЛ INHOPE;
- «Право на забвение» - из судебного прецедента превращается в европейский закон.

По теме CSAM – дискуссии относительно концепции борьбы, в результате чего должно определиться стратегия по следующим проблемам:

- «серая зона»;
- эксплуатация роботов.

GDPR и школьники

Установлен минимальный возраст регистрации в соцсетях – 16 лет (национальный законодатель может уменьшить до 13), но сохраняются возможности для обхода;

Любая возможность косвенного установления личности – персональные данные, применимость законодательства о персональных данных, включая требование об удалении информации и штрафы за отказ (в % от мирового оборота);

Пользователь должен иметь четкую информацию, для чего собираются персональные данные, как они будут использоваться и кому могут передаваться (если передаются) – для любых сервисов, осуществляющих сбор персональных данных;

GDPR распространяется на все виртуальное пространство Евросоюза, т.е. и на американские онлайн-сервисы (Microsoft, Google, Facebook)

«Пиковые» проявления угроз

Тема фейковых новостей – всплеск активности в конце 2016 года:

- Информационно-просветительская работа по фейковым новостям и фактчекингу;
- Отсутствие механизма по прекращению оборота такого контента, т.к. защищено свободой слова.

Проблема получила симптоматический всплеск в связи с выборами президента США и победой Трампа, просветительские материалы носили политизированный характер и вскоре сошли на нет.

«Blue Whale Challenge» – определенный интерес в первой половине 2017 года:

- Различные стратегии информационного противостояния;
- Оперативное установление взаимодействия с Интернет-индустрией;
- Небольшие объемы, в настоящее время в качестве масштабной проблемы не упоминается.

Личная безопасность

Отдельная проблематика – взаимосвязь эксплуатации детей с их исчезновениями и торговлей детьми. Преимущественно разрабатывается в Северной Америке, подход транслируется на Австралию и, с меньшим успехом, на Латинскую Америку.

ОБСЕ – пристальное внимание на онлайн как инструмент рекрутинга и совершения сделок с детьми как объектами;

Кросс-чекинг по базам пропавших и эксплуатируемых детей для установления личности и по возможности местонахождения;

Использование «онлайн-следа» для установления местонахождения, НО – «просвещенные» дети принимают свои меры предосторожности (удаление аккаунтов, оставление мобильных телефонов и т.п.);

Единая база данных по пропавшим детям, необходимость распространения инструментария на «темный сектор» торговли детьми. Программно-техническая основа для трансграничного обмена ориентировками.

Спасибо за внимание ☺

Урван Парфентьев,
Координатор Центра безопасного Интернета

РОЦИТ

ЦЕНТР БЕЗОПАСНОГО ИНТЕРНЕТА
ФОНД “НЕ ДОПУСТИ!”