УДК 004.056

# УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ КОРПОРАЦИИ НА УРОВНЕ РИСК-АНАЛИЗА СЕТЕВОЙ АКТИВНОСТИ ЕЕ СОТРУДНИКОВ

**И.А. Боков**
*Воронежский государственный технический университет*
Россия, 394049, Воронеж, ул. Ватутина, 1
E-mail: bokoff.il@gmail.com

**Ключевые слова:** контент, безопасность, риски, социальные сети, вероятность, регламент, база знаний.

**Аннотация:** В данном исследовании представлен новаторский подход к укреплению информационной безопасности корпоративных систем, акцентирующий внимание на риски, связанные с социотехническими атаками на персонал корпорации в контексте социальных сетей. Работа охватывает разработку и применение комплексного методического, алгоритмического и программного обеспечения для автоматизированного мониторинга, классификации и риск-анализа деструктивного контента, циркулирующего в таких социальных сетях. В результате был разработан уникальный программный комплекс, способствующий эффективному мониторингу сетевой активности сотрудников и идентификации потенциально опасного контента. Ключевым новшеством является создание обширной базы знаний о сценариях социотехнических атак и методиках их противодействия в формате регламентов, интегрированной в нейросетевой инструментарий для поддержки принятия решений.

## 1. Введение

В современном мире, где цифровые технологии проникают в каждый аспект нашей жизни, вопросы информационной безопасности становятся критически важными. Наблюдается не только увеличение количества кибератак, но и их усложнение, особенно в случаях, когда злоумышленники используют социотехнические методы для воздействия на персонал организаций. В этой динамической и многоаспектной среде становится очевидной необходимость разработки и внедрения новых подходов и инструментов для защиты корпоративных систем.

Традиционные методы обеспечения кибербезопасности, сфокусированные на технических аспектах и обороне периметра, уже не достаточны. Важно учитывать человеческий фактор, особенно в контексте социальных сетей, где персонал корпораций часто становится целью для социотехнических атак [1]. Данное исследование направлено на разработку комплексного подхода к анализу, классификации и риск-анализу деструктивного контента в социальных сетях, а также на формирование базы знаний и разработку инструментов для эффективного реагирования на соответствующие угрозы [2].

## 2. Целеполагание

С учетом изложенного выше представляется возможным сформулировать:

- **объект исследования**, как графический, аудио-, видеоконтент, циркулирующий в ресурсах социальных сетей и аффилированный с персоналом рассматриваемой корпорации;
- **предмет исследования** как процесс выявления, сбора, классификации публикаций и риск-анализа деструктивных контентов для выработки рекомендаций и регламентов по разграничению доступа к корпоративной инфраструктуре;
- **цель исследования**, состоящую в повышении защищенности атакуемых корпоративных систем за счет разработки и применения методического, алгоритмического и программного обеспечения автоматизации мониторинга, классификации, риск-анализа и регламентации противодействия социотехническим атакам.

Отсюда вытекает **научно-техническая задача** настоящей работы, заключающаяся в создании автоматизированного инструментария для управления корпоративной информационной безопасностью посредством анализа сетевой активности персонала, в том числе публикационной, и регламентации процесса реагирования на инциденты, вызванные атакой.

Исследование аналогов [3-6] позволяет констатировать наличие следующих противоречий между:

- несовершенством корпоративных систем защиты информации (а именно: отсутствие высокопроизводительных модулей мониторинга циркулирующего в социальных сетях и аффилированного с персоналом организации деструктивного контента; использование моделей нарушителя, не учитывающих социотехнические атаки и уязвимости связанные с восприятием деструктивной информации сотрудниками, а также последующие за ним невиртуальные действия; полное игнорирование социальных медиаплатформ как элементов поверхности атаки; необоснованное исключение особенностей связанных с распространением деструктивного контента из методик оценки ущерба от успешной социотехнической атаки; отсутствие инструментария выявления, классификации, оценки опасности деструктивного контента в зависимости от его типа и среды распространения) и необходимостью исправления вышеперечисленных недостатков в современных инструментах комплексной оценки информационной безопасности;
- отсутствием обобщенной и актуальной базы знаний по техникам, тактикам, мерам противодействиям, структурным и техническим особенностям, методикам обнаружения социотехнических атак, осуществляемых посредством целенаправленного и длительного воздействия деструктивным контентом на сознание персонала корпорации через социальные сети и практической потребность агрегирования и периодической актуализации вышеуказанных баз знаний и данных в виде четко регламентированных, стандартизованных процессов реагирования, расследования причин инцидентов и ликвидации их.

Представленные выше противоречия обуславливают необходимость решения следующих **задач**:

- разработка методического, алгоритмического и программного обеспечения мониторинга, выявления, интеллектуальной классификации в соответствии с тематической направленностью деструктивного графического, аудио- и видеоконтента, аффилированного с сотрудниками корпорации с последующим его рассмотрением в качестве элемента социотехнической атаки и анализом рисков воздействия на корпоративные системы;
- в формировании, поддержании в актуальном состоянии структурированных баз знаний и данных, содержащих основные тактики, техники, регламентированные методики реагирования на инциденты и ликвидации вызванных ими последствий и

последующей разработке интеллектуальных систем поддержки принятия решений в отношении доступа персонала к корпоративным информационным активам.

# 3. Результаты

Решение перечисленных задач достигнуто в форме следующих **результатов**:

- программный комплекс, обеспечивающий автоматизированный мониторинг сетевой активности сотрудников корпорации, в том числе публикационной, предоставляющий администратору корпоративных систем набор нейросетевого инструментарий по выявления и классификации деструктивного контента в зависимости от его типа (видео-, аудиозапись, графика) и тематической направленности, а также повышающий эффективность процесса комплексной оценке защищенности корпорации, за счет риск-анализа вышеуказанного контента;
- база знаний, содержащая информацию о сценариях, методах и тактиках, используемых в социотехнических атаках на корпоративные системы, структурированная в форме детализированных регламентов (регламенты охватывают различные стадии борьбы с кибератаками, включая меры по реагированию на инциденты и процедуры по устранению их последствий) и разработанный на основе этой базы знаний специализированный интеллектуальный инструментарий, поддерживающий процесс принятия решений.

**Новизна** результатов заключается в том, что:

- разработанный программный комплекс выводит на принципиально новый уровень подход к оценке защищенности информационных систем корпорации, в отличие от аналогов, учитывающий особенности генерации и циркуляции деструктивного контента, а также его влияние на корпоративные системы через негативное воздействие на сознание персонал;
- впервые предлагается сформировать базу знаний и разработать на ее основе нейросетевой инструментарий, предлагающий лицу, принимающему решения, регламенты реагирования на компьютерные инциденты и ликвидации их последствий в зависимости от типа, тематики, степени воздействия на персонал и среды распространения деструктивного контента.

**Практическая ценность** достигнутых результатов состоит в том, что:

- методика и разработанный программный комплекс позволит проводить количественную оценку рисков и дополняет собой качественные оценки, полученные на базе опросов, собеседований, что поможет сформировать наиболее полную картину ландшафта угроз, связанных с сетевой активностью персонала корпорации;
- модуль интеллектуальной поддержки, как и база регламентов, позволит частично автоматизировать работу лица, принимающего решения, в отношении доступа персонала к информационным активам корпорации, тем самым значительно снизит влияние человеческого фактора при построении и управлении инструментами защиты.

**Теоретическая значимость** результатов работы является существенной в следующих аспектах:

- методика риск-анализа, применяемая в предложенном программном комплексе, объективно имеет потенциал к совершенствованию и может быть развита, в плане учета множества категорий и типов деструктивного контента и расширения учитываемых при защите корпоративных систем факторов;

- в контексте современной практики защиты корпоративных информационных систем, создаваемая база знаний и интеллектуальный инструментарий поддержки принятия решений имеет перспективу своего теоретического развития в плане реализации машинного обучения и расширения области применения нейросетевых технологий в вопросах противодействия социотехническим атакам.

# 4. Заключение

В рамках данного исследования была предпринята значительная попытка систематизировать и анализировать проблематику социотехнических атак через персонал в корпоративной среде. Уникальность работы заключается в её масштабном и всестороннем подходе к разработке инструментария для мониторинга, классификации и риск-анализа деструктивного контента в социальных сетях, а также в создании базы знаний и инструментов для эффективного реагирования на инциденты.

Результаты исследования предоставляют ценные теоретические и практические вклады в научно-техническое сообщество, подчеркивая важность комплексного подхода к защите информационных систем от социотехнических угроз и предлагая конкретные решения для улучшения защищенности корпоративных систем.

Следует признать, что, несмотря на значительные успехи, еще существуют аспекты, требующие доработки. Тем не менее, реализация такого комплексного и актуального исследования, вносящего вклад в развитие техник и методов противодействия кибератакам, заслуживает высокой оценки.

## Список литературы

1. Остапенко А.Г., Белов Е.Б., Калашников А.О. и др. Социальные сети и психологическая безопасность / Под ред. Академика РАН Д. А. Новикова. Горячая линия – Телеком, 2020. 300 с.
2. Остапенко Г.А., Щербакова Д.В., Калашников А.О. и др. Организационно-правовая защита сетей / Под ред. Академика РАН Д. А. Новикова. Горячая линия – Телеком, 2023. 228 с.
3. ObserveIT Enterprise. http://www.infobezpeka.com/products/dlp/ObserveIT_Enterprise/.
4. Сравнительный обзор российских DLP-систем. https://falcongaze.com/ru/pressroom/publications/researchсравнительный-обзор-российских-dlp-систем.html
5. Обзор DLP-систем: как выбрать, ТОП лучших программ. https://инсайдер.рф/news/dlp_sistema_obzor_luchshikh_programm/.
6. Сетевые DLP-системы. https://www.anti-malware.ru/security/network-dlp.