СЛЕДСТВЕННЫЙ КОМИТЕТ РОССИЙСКОЙ ФЕДЕРАЦИИ

МОСКОВСКАЯ АКАДЕМИЯ СЛЕДСТВЕННОГО КОМИТЕТА

ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

Материалы международной научно-практической конференции

(Москва, 28 апреля 2023 года)

Москва, 2023

УДК 343
ББК 67.5

П 78 **Проблемы противодействия киберпреступности:** материалы международной научно-практической конференции (Москва, 28 апреля 2023 г.). М.: Московская академия Следственного комитета Российской Федерации, 2023. – 255 с.

Сборник сформирован по материалам, представленным на международную научно-практическую конференцию, проведённую в Московской академии Следственного комитета Российской Федерации 28 апреля 2023 года. Конференция организована с участием учёных, сотрудников правоохранительных органов России, профессорско-преподавательского состава и аспирантов ВУЗов.

Сборник представляет интерес для обучающихся в Академии, студентов юридических ВУЗов, юристов – учёных и практиков.

Редакционная коллегия обращает внимание на то, что научные подходы, идеи, и взгляды, изложенные в статьях сборника, отражают позиции и оценки их авторов и могут отличаться от мнения редакторов.

наук информационного блока, выверенным с правовой точки зрения. Такой подход полностью отвечает установкам государственной политики по созданию новой научной специальности 5.1.4 «Уголовно-правовые науки». При этом интегрирующую роль в создания нового инструментария в борьбе с киберэкстремизмом может взять на себя криминалистика.

Таким образом, вышесказанное определяет не только актуальность исследования проблем противодействия преступлениям экстремистской направленности, совершаемым с использованием информационно-телекоммуникационных сетей, но и его целевую установку на разработку научно обоснованных способов их разрешения и выполнение установок высшего руководства страны на формирование государственной программы борьбы с современным экстремизмом, тесно связанным с терроризмом, и его общественно опасными последствиями.

С.В. Валов

Результаты аналитических исследований субъектов кибербезопасности и реагирования на инциденты в системе информации о киберпреступности

Аннотация. Получение максимально полной информации о киберпреступности позволит всесторонне оценивать исходящие от неё угрозы и комплексно подходить к разработке мер противодействия и наступательной борьбы с различными её проявлениями в социальном пространстве в реальном и виртуальном измерениях. Дана оценка в недостаточной степени востребованной в криминологических исследованиях информации, полученной профессиональными субъектами обеспечения кибербезопасности.

Ключевые слова: киберпреступность, кибербезопасность, аналитические данные, криминологическая характеристика, показатели преступности.

На технологической основе достижений четвертой промышленной революции, предоставившей человечеству оригинальные сочетания физических, биологических и социальных систем[1], произошли качественные изменения, характеризуемые переходом от единичных случаев противоправного использования программно-аппаратных средств до не знающей государственных границ киберпреступности[2].

Масштабы противоправного воздействия киберпреступлений на различные сферы социальной жизни привели к тому, что сформировался автономный от правоохранительных органов сегмент, в котором действуют субъекты, профессионально осуществляющие функции обеспечения кибербезопасности и защиты определённых интересов, прав и свобод индивидуальных и

[1] Шваб, К. Четвертая промышленная революция. М.: «Эксмо», 2016.

[2] Герке, М. Понимание киберпреступности: Явление, задачи и законодательный ответ // Электронный ресурс. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_R.pdf <дата обращения: 26.04.2023>.

коллективных пользователей современных информационно-коммуникационных и иных цифровых технологий. Если правоохранительные органы действуют в киберпространстве во исполнение возложенных на них публичных функций, то субъекты, оказывающие услуги комплексной защиты и оперативного реагирования на инциденты в сфере обеспечения кибербезопасности, преследуют коммерческие интересы, поскольку предлагаемые ими решения и продукты востребованы на рынке. По экспертным оценкам, в настоящее время на российском рынке действует 230 отечественных компаний-разработчиков продуктов и поставщиков услуг в сфере информационной безопасности в следующих сегментах: «Защита инфраструктуры», «Мониторинг, исследование и анализ», «Защита данных» и «Услуги и сервисы»[1]. В каждом сегменте выделены специализированные направления оказания услуг. Отдельные игроки представлены во всех сегментах.

Из субъектов, которые предоставляют для публичного обозрения результаты проведённых ими аналитических исследований состояния и изменений противоправных посягательств, мотивации и технологической оснащённости киберпреступности, реальной и виртуальной географии направленности атак и расположения очагов активности, выделим аналитические исследования Kaspersky[2], «Ростелеком-Солар»[3]; Positive Technology[4], IB-Group[5] (в 2023 г. в России ребрендинг в F.A.C.C.T.[6]). Учитывая трансграничный характер глобального информационного поля, в контексте рассматриваемой проблемы обратим внимание на иностранные аналитические исследования тенденций и трендов трансформации киберпреступности[7].

Все доступные для публичного доступа аналитические материалы подразделены по степени охвата объекта исследования на *глобальные*[8] и *тематические*. В основу тематических обзоров положены различные критерии.

---

[1] Карта российского рынка информационной безопасности 2023 года // Электронный ресурс. URL: https://www.tadviser.ru/index.php/Статья:Карта_российского_рынка_. информационной_безопасности_2023 <дата обращения: 26.04.2023>.

[2] https://www.kaspersky.ru/blog/category/threats/ <дата обращения: 26.04.2023>.

[3] https://rt-solar.ru/analytics/reports/ <дата обращения: 26.04.2023>.

[4] https://www.ptsecurity.com/ru-ru/research/analytics/ <дата обращения: 26.04.2023>.

[5] https://www.group-ib.com/resources/research-hub/ <дата обращения: 26.04.2023>.

[6] https://www.facct.ru/resources/research-hub/ <дата обращения: 26.04.2023>.

[7] См., например: https://www.cyderes.com/blog/category/resources/ <дата обращения: 20.05.2023>.

[8] См.: Актуальные киберугрозы: итоги 2022 года / Positive Technology, 29 марта 2023 года // Электронный ресурс. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/ <дата обращения: 26.04.2023>; Эволюция киберпреступности. Анализ, тренды и прогнозы 2022/2023 / Ежегодный флагманский отчёт Group-IB // Электронный ресурс. URL: https://www.facct.ru/resources/research-hub/hi-tech-crime-trends-2022/ <дата обращения: 26.04.2023>; 2022 cybersecurity conversations report // Электронный ресурс. URL: https://www.cyderes.com/wp-content/uploads/2022/07/2022-Cybersecurity-Conversations-Report_V1.0.pdf <дата обращения: 26.04.2023>.

К ним отнесены государства[1], сектора и сегменты мировой[2] или региональной экономик[3], государственного управления[4], оказания целевых услуг населению, виртуальные социальные пространства; технологии, используемые в противоправных целях, и модели их применения в отношении определённых групп объектов; имущественный и репутационный вред, причинённый кибератаками[5]; уязвимости операционного и прикладного обеспечения; стратегии создания и обеспечения целостности контура безопасности; алгоритмы действий специалистов в области кибербезопасности на прогнозируемые и состоявшиеся инциденты; возможности установления лиц, виновных в кибератаках на объекты посягательства[6].

По временным параметрам аналитические отчёты подразделены на *годовые* и *периодические*. Во второй группе выделим ежеквартальные отчёты об актуальных киберугрозах в отношении определённых объектов. Выстроенные в хронологическом порядке они позволяют с большей точностью отслеживать происходящие изменения и анализировать оперативность реагирования заинтересованных субъектов в публичном и частном секторе на причины проявления активности и наступившие негативные последствия.

По направленности фокуса внимания выделим *диагностические*, *прогностические*[7] и *комплексные* отчёты. В первых внимание уделяют причинам возникновения и процессу проявления конкретных угроз, во второй группе – предприняты попытки выстроить модель уязвимостей, направления, средства и методы атак на защищаемые ценности, выстроить стратегии и определить тактику противодействия, в третьей – события прошлого, настоящего и будущего рассмотрены во временной и логической последовательности.

В обзорах представлены следующие параметры, характеризующие современное состояние девиантных проявлений в киберпространстве: 1) общее число зарегистрированных инцидентов; 2) соотношение успешных и отражённых атак; 3) выбор объекта атак (индивиды или организации,

---

[1] Cyber crime in India – statistics & facts // Электронный ресурс. URL: https://www.statista.com/topics/5054/cyber-crime-in-india/ <дата обращения: 20.05.2023>.

[2] Healthcare Cybersecurity Report 2021-2022 // Электронный ресурс. URL: https://www.cyderes.com/blog/cybersecurity-healthcare-report-2021-2022/ <дата обращения: 20.05.2023>.

[3] Как атаковали российский бизнес в 2022 году // Электронный ресурс. URL: https://www.facct.ru/resources/research-hub/incident-response-2022/ <дата обращения: 26.04.2023>.

[4] Отчет об исследовании серии кибератак на органы государственной власти РФ // Электронный ресурс. URL: https://rt-solar.ru/analytics/reports/2203/?ysclid=lhwbznchkq326878276 <дата обращения: 26.04.2023>.

[5] Техники и тактики киберпреступников // Электронный ресурс. URL: https://rt-solar.ru/analytics/reports/3416/ <дата обращения: 26.04.2023>.

[6] Возможности мобильной криминалистики: как извлекать и исследовать данные мобильных устройств и раскрывать преступления // Электронный ресурс. URL: https://www.facct.ru/resources/research-hub/mobile-forensics/ <дата обращения: 26.04.2023>.

[7] URL: https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf <дата обращения: 26.04.2023>.

государственный сектор, IT-компании, отдельные сектора экономики); 4) используемые технологии и тактика действий злоумышленников (фишинг, бреши в операционных системах, уязвимости в компонентах программ, средства аутентификации клиента); 5) предмет интереса злоумышленников (персональные данные, данные платёжных карт, вэб-сайты для коммуникации с клиентами, электронные деньги, нарушение логистики товаров и информации, устойчивость систем защиты, оперативность реагирования на проникновение и др.). По оценкам экспертов Positive Technology в 2022 году чаще всего конфиденциальная информация была похищена в медучреждениях (в 82% инцидентов), в научных и образовательных организациях (в 67%), в ритейл-сегменте (в 65%)[1] для последующего использования с учётом достижений социальной инженерии и оказания влияния на объект воздействия.

Резонно возникает вопрос об обоснованности представленных результатов. В пользу говорят использованные методы, которые авторы не скрывают. К ним отнесены обобщение сведений о расследованных инцидентах, сопоставление результатов с данными конкурентов, опросы лиц, ответственных за кибербезопасность в различных организациях. К факторам, требующим критической оценки, отнесём охват вниманием любых инцидентов без использования норм уголовного законодательства, коммерциализацию оказываемых услуг, решение задач роста их востребованности на фоне представленной картины досягаемости и уязвимости от атак. В целях противодействия в получении информации противной стороной отдельные субъекты предоставляют сведения только персонифицированным потребителям, действия в сети и аутентичность которых могут быть перепроверены.

Изложенная в обзорах информация даёт возможность при её всесторонней обработке и многократной проверке получить достаточно полное представление о ландшафте современных угроз, оценить степень их общественной опасности, скорректировать нормативные модели деяний, преследуемых государством в различных правовых режимах, актуализировать методики расследования преступлений, разработать новые тактические приёмы. Интерес вызывают методика и приёмы изложения представляемых сведений. Одновременно аналитические отчёты позволяют задуматься о пересмотре устоявшейся системы абсолютных и относительных криминологических показателей преступности с учётом социальных процессов, присущих исключительно киберпреступлениям.

Литература

1. Актуальные киберугрозы: итоги 2022 года / Positive Technology, 29 марта 2023 года // Электронный ресурс. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/ <дата обращения: 26.04.2023>.
2. Возможности мобильной криминалистики: как извлекать и исследовать данные мобильных устройств и раскрывать преступления // Электронный

[1] Актуальные киберугрозы: итоги 2022 года.

ресурс. URL: https://www.facct.ru/resources/research-hub/mobile-forensics/ <дата обращения: 26.04.2023>.
3. Герке, М. Понимание киберпреступности: Явление, задачи и законодательный ответ // Электронный ресурс. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_R.pdf <дата обращения: 26.04.2023>.
4. Как атаковали российский бизнес в 2022 году // Электронный ресурс. URL: https://www.facct.ru/resources/research-hub/incident-response-2022/ <дата обращения: 26.04.2023>.
5. Карта российского рынка информационной безопасности 2023 года // Электронный ресурс. URL: https://www.tadviser.ru/index.php/Статья: Карта_российского_рынка_информационной_безопасности_2023 <дата обращения: 26.04.2023>.
6. Отчёт об исследовании серии кибератак на органы государственной власти Российской Федерации // Электронный ресурс. URL: https://rt-solar.ru/analytics/reports/2203/?ysclid=lhwbznchkq326878276 <дата обращения: 26.04.2023>.
7. Техники и тактики киберпреступников // Электронный ресурс. URL: https://rt-solar.ru/analytics/reports/3416/ <дата обращения: 26.04.2023>.
8. Шваб, К. Четвертая промышленная революция. М.: «Эксмо», 2016.
9. Эволюция киберпреступности. Анализ, тренды и прогнозы 2022/2023 // Электронный ресурс. URL: https://www.facct.ru/resources/research-hub/hi-tech-crime-trends-2022/ <дата обращения: 26.04.2023>.
10. Cyber crime in India – statistics & facts // Электронный ресурс. URL: https://www.statista.com/topics/5054/cyber-crime-in-india/ <дата обращения: 20.05.2023>.
11. Healthcare Cybersecurity Report 2021-2022 // Электронный ресурс. URL: https://www.cyderes.com/blog/cybersecurity-healthcare-report-2021-2022/ <дата обращения: 20.05.2023>.

А.А. Вихляев

О некоторых мерах по мониторингу информационно-телекоммуникационных сетей при реализации комплексных мероприятий, направленных на выявление и раскрытие преступлений, связанных с распространением религиозных материалов экстремистской направленности

Аннотация. В рамках исследования обозначенной проблематики, автором проведен анализ современной системы противодействия религиозному экстремизму в информационно-телекоммуникационных сетях. На основе полученных данных обозначены наиболее актуальные меры, позволяющие обеспечить действенный мониторинг религиозно-экстремистского контента в сети «Интернет» через призму текущей криминологической и общественно-политической ситуации. Также в статье дана фактическая оценка реализации

Содержание