ПЕРМСКИЙ
ГОСУДАРСТВЕННЫЙ
НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное
образовательное учреждение высшего образования
«ПЕРМСКИЙ ГОСУДАРСТВЕННЫЙ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ»

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Сборник статей

Выпуск 1

Пермь 2025

УДК 004
ББК 32.81
А437

Актуальные проблемы информационной безопасности = Current information security issues [Электронный ресурс] : сборник статей / Пермский государственный национальный исследовательский университет. – Электронные данные. – Пермь, 2025. – Вып. 1. – 3,64 Мб; 147 с. – Режим доступа: http://www.psu.ru/files/docs/science/books/sborniki/aktualnye-problemy-informacionnoj-bezopasnosti-2025.pdf. – Заглавие с экрана.

ISBN 978-5-7944-4227-4

Сборник содержит статьи, посвященные различным проблемам информационной безопасности, являющимся наиболее актуальными в настоящее время в Российской Федерации. Данный выпуск сборника отражает результаты исследований по вопросам информационной безопасности, проводимых на различных предприятиях и в организациях Пермского края.

Материалы сборника предназначены для специалистов в области информационной безопасности.

The collection contains articles devoted to various problems of information security, which are the most topical at present in the Russian Federation. This issue of the collection reflects the results of research on information security issues, conducted at various enterprises and organizations of Perm Krai.

The materials of the collection are intended for specialists in the field of information security.

УДК 004
ББК 32.81

Издается по решению института компьютерных наук и технологий Пермского государственного национального исследовательского университета

Редакторы:
Е. А. Рабчевский (ответственный редактор),
Н. И. Григоров, Е. Ю. Никитина, А. Н. Рабчевский, А. В. Черников

Editors:
E.A.Rabchevsky (responsible editor),
N. I. Grigorov, E. Yu. Nikitina, A. N. Rabchevsky, A. V. Chernikov

Рецензенты: и. о. зав. кафедрой прикладной информатики, информационных систем и технологий ПГГПУ, канд. техн. наук ***А. Г. Кузнецов;***
д-р техн. наук, профессор ***О. Г. Пенский***

ISBN 978-5-7944-4227-4

ОГЛАВЛЕНИЕ

ИНФОРМАЦИОННОЕ ПРОТИВОБОРСТВО КАК ЭЛЕМЕНТ СТРАТЕГИЧЕСКОГО ВЗАИМОДЕЙСТВИЯ МЕЖДУ ГОСУДАРСТВАМИ

Х.М. Абдиев, А.А. Некрасов
Пермский военный институт войск национальной гвардии РФ

Аннотация. В данной статье анализируется понятие информационного противоборства как элемент стратегического взаимодействия между государствами, включая геополитические измерения информационного противоборства. Приводятся примеры обновления стратегий государственной политики в ответ на изменения в информационном пространстве. Показываются примеры применения информационного противоборства.
Ключевые слова: *информационное противоборство, государство, геополитические измерения, информационное пространство, информационная война, дезинформация, кибербезопасность, киберпространство.*

Информационное противоборство – соперничество социальных систем в информационно-психологической сфере с целью усиления влияния на те или иные сферы социальных отношений и установления контроля над источниками стратегических ресурсов, в результате которого одни участники соперничества получают преимущества, необходимые им для дальнейшего развития, а другие их утрачивают.

Сущность информационного противоборства заключается в борьбе в информационной сфере, которая предполагает комплексное деструктивное воздействие на информацию, информационные системы и информационную инфраструктуру противоборствующей стороны с одновременной защитой собственной информации, информационных систем и информационной инфраструктуры от подобного воздействия.

Цель информационного противоборства – обеспечение национальных интересов в информационно-психологической сфере, включая обеспечение геополитической и информационно-психологической безопасности государства, достижение превосходства в сфере международных отношений и другое.

Анализируя историю России с точки зрения глобальной геополитики, успех всех геополитических проектов напрямую связан с преимуществом в информационном противоборстве. Информационная война проходит в самых разных сферах жизни общества и государства – политике, экономике, культуре, религии и т.д. Примечательно, что для постиндустриальной эпохи характерна интеграция различных областей ведения информационной войны в единую смысловую и целеположенную сеть разом.

Составной частью информационной войны становится относительно новое понятие «сетевая война». Борьба за геополитическое превосходство

на всех этапах развития мировой истории ведется средствами, которые соответствуют конкретному времени. На сегодняшний момент можно сказать, что это сетевые средства, поэтому борьба развертывается в сетевом пространстве. Войны всегда отражали уровень технического развития, и в современную постиндустриальную эпоху странами Запада, в первую очередь США, активно разрабатывается модель войны нового типа. Эта теория получила название «сетевая война». Сетевая война – это теория качественного сдвига в военных технологиях и в устройстве современных обществ в целом. В России «сетевая война» рассматривается как «искусственный процесс, построенный на Западе и направленный на дестабилизацию регионов на постсоветском пространстве»

Исторически теория сетевых войн пришла на смену концепции ядерного сдерживания, которая преобладала в эпоху холодной войны и основывалась на соревновании в производстве ядерного оружия и средств его доставки на территорию вероятного противника между двумя сверхдержавами США и СССР. Сетевая война в отличие от войн предшествующего периода ведется не государствами и даже не блоками, а глобальными структурами, которые могут быть как институционализированы тем или иным образом, так и иметь подрывной террористический характер.

Цифровые технологии могут использоваться как инструменты манипуляции для воздействия на общественное мнение, личные предпочтения и даже повседневные действия людей. Один из главных инструментов – социальные сети. Алгоритмы, управляющие новостными лентами, отбирают контент, который больше всего соответствует интересам и предпочтениям конкретного пользователя. Это создаёт так называемый «пузырь фильтров», в котором человек сталкивается преимущественно с теми мнениями и идеями, которые подтверждают его собственные взгляды. Ещё один аспект манипуляции – использование эмоций. В эпоху цифровых технологий контент, вызывающий сильные эмоциональные реакции, получает большее распространение. Это связано с тем, что алгоритмы социальных сетей зачастую фаворируют материалы, способные вызвать шок, радость или гнев. Манипуляция в цифровую эпоху также используется в сфере маркетинга и рекламы. Бренды изучают поведение пользователей, собирая данные о их предпочтениях и привычках. Это знание позволяет им создавать целенаправленные рекламные кампании, которые тонко воздействуют на подсознание.

Чтобы эффективно противостоять манипуляциям, важно развивать критическое мышление, анализировать источники, проверять факты и осмысленно подходить к потреблению информации.

Адаптация стратегий в условиях изменений информационного ландшафта. Некоторые примеры обновления стратегий государственной политики в ответ на изменения в информационном пространстве: стратегия США по международному киберпространству и цифровой политике. Документ, опубликованный в мае 2024 года, основан на концепции цифровой солидарности и предусматривает позитивное видение киберпространство и

цифровых технологий, их увязку с международными обязательствами и правом, включая права человека. Также стратегия предполагает интеграцию кибербезопасности, устойчивого развития и технологических инноваций.

Стратегия развития информационного общества в России. Обновлённая стратегия, утверждённая в 2024 году, в качестве главной цели деятельности в области цифровизации называет формирование системы, обеспечивающей оперативную и эффективную передачу сведений между элементами информационного общества, в том числе между гражданами, организациями и органами власти. Стратегия научно-технологического развития Российской Федерации. Документ, утверждённый указом Президента РФ от 28 февраля 2024 года, направлен на формирование эффективной системы взаимодействия науки, технологий и производства, повышение восприимчивости экономики и общества к новым технологиям, развитие наукоёмкого предпринимательства.

Сложности адаптации военного и политического подходов к новым вызовам и угрозам, связанным с цифровой средой, отсутствие единого общепринятого на международном уровне определения понятий «информационная угроза» и «киберугроза». Это ограничивает эффективность межгосударственного сотрудничества и усложняет разработку стратегий противодействия киберугрозам. Асимметричность ситуации заключается в том, что хорошо оснащённые технически вооружённые силы становятся ещё одной уязвимостью, в то время как слабо организованные вооружённые формирования не имеют такой проблемы.

Отсутствие правоприменительных практик в международных отношениях, регулирующих использование киберпространства для агрессивных действий. Это важно, поскольку создаваемые образцы кибероружия отличаются глобальной досягаемостью и практически мгновенным воздействием.

Трудности в психологической адаптации военнослужащих. В условиях современных военных конфликтов они сталкиваются с огромным объёмом информации, часть которой может быть искажённой, противоречивой или даже враждебной. Это создаёт специфические трудности в области психологической защиты и поддержки. Для успешной адаптации к новым вызовам и угрозам, связанным с цифровой средой, необходимы совместные усилия военных психологов, специалистов по информационной безопасности и технических экспертов, а также поддержка со стороны высшего военного руководства.

Примеры применения информационного противоборства. Информационная политика стран НАТО в период обострения вооружённого конфликта в Косово (Югославия, 1999 год) и Ираке (2003 год). На глобальном уровне страны НАТО пытались убедить международное общественное мнение в том, что в Югославии, Афганистане, Ираке совершается геноцид в отношении некоторых национальных, религиозных и социальных групп. На региональном уровне воздействие было направлено на дестабилизацию и обострение внутриполитического положения в странах и в зоне конфликта, деморализацию населения и вооружённых сил.

Захват заложников в Греции 15 декабря 2004 года. Весь день мировые СМИ, в том числе и ряд российских СМИ, тиражировали фальшивые сообщения о том, что якобы россияне захватили автобус с заложниками в Греции. К концу дня всем стало ясно, что террористы – албанские, ранее неоднократно судимые.

Грузино-югоосетинский конфликт. Многие эксперты считают, что в этом конфликте роль информационной составляющей возросла. Например, при голосовании на сайте CNN, где предлагалось оценить действия России по отношению к Грузии, накрутка голосов способствовала признанию поведения России миротворческим.

Методы борьбы с дезинформацией:

1. Алгоритмы машинного обучения. Они помогают анализировать текст и контент, выявлять аномалии и несоответствия в информации.

2. Технологии детекции дипфейков. С их помощью можно обнаруживать поддельные изображения и видео.

3. Повышение медиаграмотности и критического мышления. Способность анализировать и оценивать информацию помогает пользователям распознавать манипуляции и принимать информированные решения.

4. Сетевой анализ и выявление фальшивых аккаунтов в социальных сетях. Это позволяет установить паттерны поведения, характерные для искусственного воздействия, и эффективно фильтровать такие аккаунты.

5. Фактчекинг. Анализ и проверка информации, установление её корректности и достоверности.

Важность формирования устойчивости общества к манипуляциям заключается в том, что дезинформация подрывает доверие людей к правительствам и другим общественным институтам. Ложная информация способна формировать ложные взгляды и убеждения у людей, влиять на их поведение и принятие решений.

В заключении хотелось отметить перспективы будущего информационного противоборства. Это развитие технологий. К функциям различных устройств добавится симуляция реальности, искусственный интеллект, а сами носители станут доступными и простыми в использовании. Стирание границ. Открытое и незаметное проникновение в процессы воспитания и социализации подрастающего поколения путём формирования и предоставления новой виртуальной реальности, независимого от влияния традиционных ценностей, культуры, религий. Массовое управление. Через различные аддикции: социальные сети, игры, секты, развлечения. Целенаправленное формирование субъективной реальности. В информационной войне будущего не будут иметь значение реальные события и факты, а только созданные, тиражированные, интерпретированные для целевой аудитории с учётом их потребностей, интересов, зависимостей. Объединение мировых корпораций. Возможность использовать информационную войну против государств с целью их ослабления и уничтожения.

По мнению некоторых экспертов, техническое развитие через 10–20 лет внесёт коррективы и ускорит процессы информационного противостояния, вовлекая практически всё мировое сообщество.

Список литературы

1. Бартош А.А. Модель управляемого хаоса в сфере обеспечения военной безопасности. М.: Вестник Академии военных наук № 1 (46), 2014, С. 69-78.
2. Бартош А.А Модель управляемого хаоса в культурно – мировоззренческой сфере. М.: Вестник Московского государственного лингвистического университета, выпуск № 39, 2014, С. 9-27.
3. Бартош А.А. Гибридные войны как проявление глобальной критичности современного мира – Геополитика и безопасность – №1 (29) – 2015 С 71-79.
4. Алексеев А.П., Алексеева И.Ю. Информационная война в информационном обществе // Вопросы философии. 2016. № 11.

Завадский И.И. Информационная война – что это такое? // Защита информации. № 4, 1996. EDN WZTMBZ

5. Иванов Д. В. Виртуализация общества [Текст]: Версия 2.0 / Д. В. Иванов. – СПб.: Петербургское востоковедение, 2002. – 217 с. Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве.
6. Манойло А.В., Петренко А.И., Фролов Д.Б. Государственная информационная политика в условиях информационно – психологической войны. 3-е изд. М.: Горячая линия – Телеком, 2012. ISBN 978-5-9912-0253-4 EDN PISZON

INFORMATION CONFRONTATION AS AN ELEMENT OF STRATEGIC COOPERATION BETWEEN STATES

H.M. Abdiev, A.A. Nekrasov
Perm Military Institute of the National Guard Troops of Russian Federation.

Abstract. This article analyzes the concept of information confrontation as an element of strategic interaction between states, including «geopolitical dimensions of information confrontation». Examples of updating public policy strategies in response to changes in the information space are given. Examples of the use of information confrontation are shown.
Keywords: *information confrontation, geopolitical dimensions, information state, space, information warrior, disinformation, cybersecurity, cyberspace.*

АВТОМАТИЗАЦИЯ ГЕНЕРАЦИИ КОММЕНТАРИЕВ С ИСПОЛЬЗОВАНИЕМ НЕЙРОСЕТИ «CHATGPT»

А.Д. Байбакова, И.В. Подюков, Н.С. Соколов,
К.Ю. Сухих, А.Н. Рабчевский
Пермский государственный национальный исследовательский университет

Аннотация. В исследовании предложен метод автоматизации процесса генерации комментариев в социальной сети «ВКонтакте» на естественном языке с использованием «ChatGPT». Данный подход обеспечивает возможность создания комментариев с различными оттенками и содержанием. Результаты последующих аналитических исследований показали, что данный метод может быть использован кибервойсками в информационном противоборстве.
Ключевые слова: *информационные войны, информационное противоборство; промпты, ChatGPT.*

Введение

Сегодня наблюдается увеличение направленности на создание информационного общества, которое заменяет индустриальное. Применение современных информационно-коммуникационных технологий одним государством с целью получения превосходства над другим приводит к различным проявлениям актов информационной войны.

Согласно проекту Конвенции об обеспечении информационной безопасности ООН [1], информационная война, это «межгосударственное противоборство в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам; для подрыва политической, экономической и социальной систем; массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны».

В условиях информационной войны на первый план выходит информационное противоборство. Информационное противоборство – форма межгосударственного противоборства, предусматривающая целенаправленное использование специально разработанных средств для воздействия на информационный ресурс противостоящей стороны и защиты собственных ресурсов в интересах достижения поставленных политических и военных целей [2]. Частью информационного противоборства является активное информационное противодействие в виде распространения противодействующего контента. Большая часть информационного воздействия осуществляется через социальные сети. Внедрение контента происходит с помощью публикации постов, его распространение в виде репостов. Лайки

используются для повышения доверия пользователей к распространяемой информации, а с помощью комментариев можно поддерживать интерес к теме. Однако для обеспечения широкой волны обсуждений требуется большое количество операторов, что является серьезным препятствием ввиду недостатка персонала. Так как социальная сеть «ВКонтакте» охватывает максимальную аудиторию российских пользователей, она является одной из основных площадок, где разворачиваются самые масштабные информационные войны, поэтому поддержание интереса пользователей к темам постов противодействующего контента является одной из важнейших задач информационного противоборства. В связи с этим актуальной является задача автоматизации процесса генерации комментариев в социальной сети «ВКонтакте».

Обзор литературы

Комментарии являются формой дискуссии или диалога, в случае двух участников. Следовательно, интерес представляют технологии, позволяющие генерировать тексты, имитирующие общение между живыми людьми. Проблемы обработки естественного языка (NLP) давно исследуются в научном сообществе, однако последние достижения архитектуры GPT [3] показывают ее превосходные генеративные способности. Проблемам автоматической генерации диалога посвящено множество работ. Специалисты Сбербанка предлагают такое решение проблемы: они создали семейство виртуальных ассистентов «Салют», в основе которого лежит RU GPT3, а также база заготовленных редакторских ответов [4].

Также движок диалоговых систем RASA, при помощи современных методов глубокого обучения, позволяет создавать чат-боты для различных предметных задач. Разговорный чат-бот Rasa Core создан на основе Rasa Stack и Python. Rasa Core – управление диалогами. Для обучения чат-бота диалогами используются 4 компонента: Домен (domain.yml), Истории (stories.md), Политики (policy.yml), Пользовательские действия (actions.py) [5].

Наука о данных (Data Science) позволяет извлекать ценную информацию из огромных объемов данных при помощи статистических и вычислительных методов. В публикации [6] представлен пример создания ИИ ассистента на базе ChatGPT и Streamlit (веб-фреймворк, предназначенный для исследователей данных для простого развертывания моделей и визуализацией с использованием Python).

Компания «Аватар Машина» создала первого в России цифрового психолога – генеративного чат бота Сабина Ai. В основе бота лежит одна из моделей GPT-like(ChatG PT3) и наработки компании по улучшению генеративных ответов модели. [7].

«Яндекс» добавил нейросеть нового поколения под названием YandexGPT (YaGPT) в виртуальный помощник «Алиса». Данная технология работает в режиме тестирования. «Алиса» может ошибаться в фактах, что не мешает ей создавать что-то новое с помощью своей эрудиции и

умения делать выводы. В отличие от предыдущих языковых моделей, нейросеть YandexGPT дообучили на сотнях тысяч примеров содержательных и хорошо написанных ответов. Именно поэтому она отвечает так же просто и понятно, как знающий человек. Для активации опции генерации текста с помощью нейросети YandexGPT достаточно сказать: «Алиса, давай придумаем!», потом ассистенту можно ставить разные задачи, но самостоятельно она не может построить естественный диалог с нами, так как YandexGPT отвечает только на конкретно поставленный вопрос [8].

Представленные выше решения показывают феноменальные возможности поддержания видимости естественности диалога, однако ни одно из них не использовалось для интеграции в социальную сеть ВКонтакте. В связи с этим перед нами стояла задача исследовать возможности автоматической генерации комментариев в социальной сети «ВКонтакте» с помощью большой языковой модели, основанной на архитектуре GPT.

Постановка задачи

Целью данной работы было исследовать возможности автоматической генерации комментариев в социальной сети «ВКонтакте» с помощью большой языковой модели. Для достижения указанной цели необходимо было решить следующие задачи:

- Выбрать наиболее подходящую предварительно обученную (pre-trained models, PTM) модель [9];
- написать программу по автоматизации процесса генерации комментариев на основе реальных текстов построения естественного диалога;
- интегрировать программу автоматической генерации комментариев в социальную сеть «ВКонтакте»
- создать набор промптов, который эффективно поможет в генерации естественного диалога;
- проанализировать сгенерированные комментарии на предмет естественности диалога.

Метод

Социальная сеть «ВКонтакте» устроена так, что продвижение постов происходит за счёт постов и репостов, а благодаря комментариям можно поддерживать интерес аудитории. Это хороший способ быстрого распространения информации.

В связи с тем, что возникает нехватка операторов, которые нужны для обеспечения широкой волны обсуждения, было предложено реализовать данную задачу следующим способом:

Была взята PTM модель третьего поколения, а именно модель GPT-3,5, которая является версией GPT-3.

Программный код продукта был реализован на языке «python», так как в него встроены библиотеки, которые дают большие возможности.

Процесс передачи информации от соцсети «ВКонтакте» в ChatGPT, получении ответа от ChatGPT и отправки его в соцсеть «ВКонтакте» выполнялся путем объединения двух библиотек «vk» и «OpenAPI».

Для взаимодействия с социальной сетью «ВКонтакте» необходимо было создать standalone приложение, для чего по специальной ссылке был получен токен с нужными правами: создание записи на стене, ее чтение, а также доступ к аккаунту и его возможностям в любое время. Далее использовались библиотеки «vk» [10], для отправки ссылки поста на обработку и публикация комментария, то есть перенаправление ответа от ChatGPT в комментарии под постом; библиотеки «re»[11] для регулярных выражений, которая позволяет извлекать ID группы и ID записи из ссылки; библиотеки «OpenAI»[12], для получения токена, с помощью которого можно подключиться к «OpenAI» для взаимодействия с ChatGPT, а далее ввести запрос и соответственно получить ответ.

После успешного завершения технических задач по интеграции ChatGPT и «ВКонтакте», на первый план вышла задача достижения максимальной естественности комментариев, которая решалась с помощью промпт-инжиниринга**.**

Мы придерживались системы принципов составления текстовых запросов для искусственного интеллекта. С помощью перебора слов мы пытались создать наиболее точные промпты – запросы, задания в словесном виде в нейросеть [13]. Для обеспечения естественности обсуждения было определено четыре роли по типу отношений к обсуждаемой информации: нейтральная, позитивная, негативная, критик. В целях эксперимента для каждой роли был выделен отдельный аккаунт ВК. Также для каждой роли был создан отдельный словарь промптов. Сами промпты из словаря в каждой роли задавались рандомно для достижения максимального разнообразия. В результате экспериментов с подбором промптов удалось получить модель поддержания диалога. Примеры автоматически сгенерированного диалога представлены на рис.1 и 2.

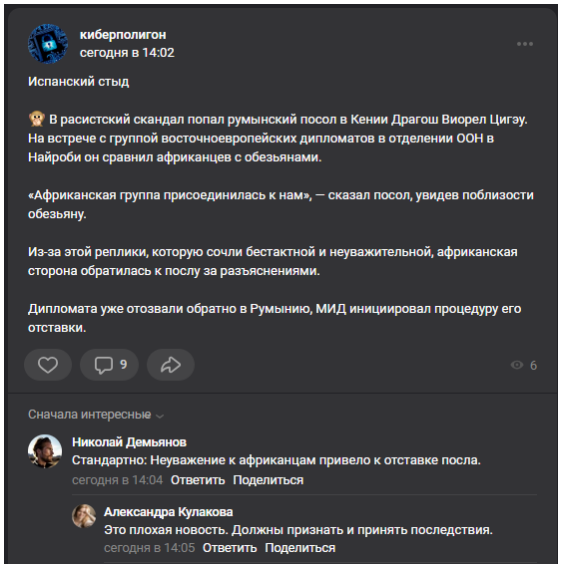

Рис. 1. Сгенерированный диалог №1

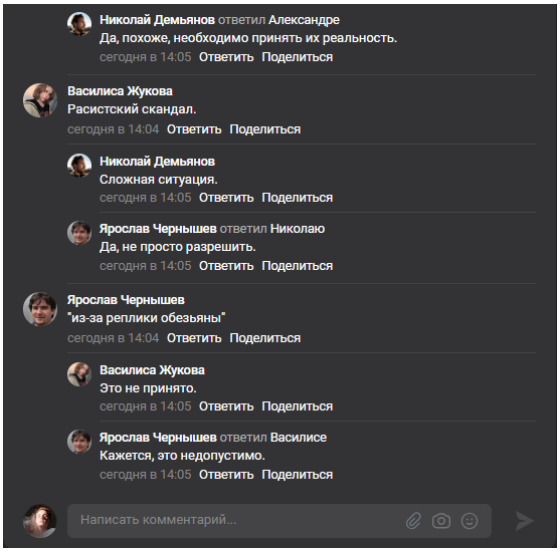

Рис. 2. Сгенерированный диалог №2

Полный перечень созданных промптов для бота с нейтральным отношением следующий:

Как ты оцениваешь эту новость? (up to 7 words)
Что тебе приходит в голову по поводу этой новости? (up to 7 words)
Какие мысли вызывает у тебя эта новость? (up to 7 words)
Что ты думаешь об этой новости? (up to 7 words)
Какие факты тебе известны насчет этой новости? (up to 7 words)
Прокомментируй новость со словом обычно (up to 7 words)
Прокомментируй новость со словом стандартно (up to 7 words)
Прокомментируй новость со словом типично (up to 7 words)
Прокомментируй новость со словом обыденно (up to 7 words)
Прокомментируй новость со словом необычно (up to 7 words)
Прокомментируй новость со словом неожиданно (up to 7 words)
Прокомментируй новость со словом интересно (up to 7 words)
Прокомментируй новость со словом неинтересно (up to 7 words)
Прокомментируй новость со словом познавательно (up to 7 words)
Прокомментируй новость со словом не очень (up to 7 words)
Прокомментируй новость со словом безразлично (up to 7 words)
Прокомментируй новость со словом нейтрально (up to 7 words)
Прокомментируй новость со словом спокойно (up to 7 words)
Прокомментируй новость со словом обычно (up to 7 words)
Прокомментируй новость со словом нормально (up to 7 words)

Словарь промптов для бота с позитивным отношением:

Как ты оцениваешь эту новость? (up to 7 words)
Что тебе нравится в этой новости? (up to 7 words)
Это замечательная новость! Ты согласен? (up to 7 words)
Какие плюсы видишь в этой новости? (up to 7 words)
Что лучше всего в этой новости? (up to 7 words)
Прокомментируй новость со словом красиво (up to 7 words)
Прокомментируй новость со словом интересно (up to 7 words)

Прокомментируй новость со словом удивительно (up to 7 words)
Прокомментируй новость со словом радостно (up to 7 words)
Прокомментируй новость со словом восхитительно (up to 7 words)
Прокомментируй новость со словом прекрасно (up to 7 words)
Прокомментируй новость со словом фантастически (up to 7 words)
Прокомментируй новость со словом потрясающе (up to 7 words)
Прокомментируй новость со словом отлично (up to 7 words)
Прокомментируй новость со словом невероятно (up to 7 words)
Прокомментируй новость со словом великолепно (up to 7 words)
Прокомментируй новость со словом превосходно (up to 7 words)
Прокомментируй новость со словом замечательно (up to 7 words)
Прокомментируй новость со словом потрясающе (up to 7 words)
Прокомментируй новость со словом необыкновенно (up to 7 words)

Словарь промптов для бота с негативным отношением:

Почему такая плохая новость? (up to 7 words)
Какие минусы ты видишь в этой новости? (up to 7 words)
Это ужасная новость! Ты согласен? (up to 7 words)
Какие проблемы возникают из-за этой новости? (up to 7 words)
Что хуже всего в этой новости? (up to 7 words)
Прокомментируй новость со словом скучно (up to 7 words)
Прокомментируй новость со словом неинтересно (up to 7 words)
Прокомментируй новость со словом обыденно (up to 7 words)
Прокомментируй новость со словом заезженно (up to 7 words)
Прокомментируй новость со словом стандартно (up to 7 words)
Прокомментируй новость со словом стерильно (up to 7 words)
Прокомментируй новость со словом банально (up to 7 words)
Прокомментируй новость со словом нелепо (up to 7 words)
Прокомментируй новость со словом неубедительно (up to 7 words)
Прокомментируй новость со словом плохо (up to 7 words)
Прокомментируй новость со словом ужасно (up to 7 words)
Прокомментируй новость со словом отвратительно (up to 7 words)
Прокомментируй новость со словом неприятно (up to 7 words)
Прокомментируй новость со словом омерзительно (up to 7 words)
Прокомментируй новость со словом гадко (up to 7 words)

Словарь промптов для бота с критическим отношением:

Что не так с этой новостью? (up to 7 words)
Какие проблемы возникают из-за этой новости? (up to 7 words)
В чем этой новости недостаток? (up to 7 words)
Можешь ли ты указать на недочеты этой новости? (up to 7 words)
Что можно было бы улучшить в этой новости? (up to 7 words)
Прокомментируй новость со словом неудачно (up to 7 words)
Прокомментируй новость со словом слабо (up to 7 words)
Прокомментируй новость со словом ошибочно (up to 7 words)
Прокомментируй новость со словом несвоевременно (up to 7 words)
Прокомментируй новость со словом неуместно (up to 7 words)

Прокомментируй новость со словом абсурдно (up to 7 words)
Прокомментируй новость со словом нелепо (up to 7 words)
Прокомментируй новость со словом посредственно (up to 7 words)
Прокомментируй новость со словом низкокачественная (up to 7 words)
Прокомментируй новость со словом дешево (up to 7 words)
Прокомментируй новость со словом неэффективно (up to 7 words)
Прокомментируй новость со словом неубедительно (up to 7 words)
Прокомментируй новость со словом непрофессионально (up to 7 words)
Прокомментируй новость со словом бездарно (up to 7 words)
Прокомментируй новость со словом негативно (up to 7 words)

Заключение

В данной работе была создана программа автоматизации процесса генерации комментариев в социальной сети «ВКонтакте» с помощью нейросети ChatGPT. Результаты использования данной программы показали, что программа успешно имитирует диалог. В то же время, нельзя не отметить и тот факт, что сгенерированные комментарии не отличаются естественностью. В связи с этим актуальным является продолжение исследований в части создания словаря промптов, обеспечивающих максимальную естественность диалога. Тем не менее, при условии использования достаточно большого количества аккаунтов, от имени которых ведется диалог, и подготовки более совершенных промптов, предложенный метод автоматической генерации диалога в социальной сети может быть признан весьма перспективным.

Список литературы

1. Концепция Конвенции ООН об обеспечении международной информационной безопасности // Совет Безопасности Российской Федерации. URL: http://www.scrf.gov.ru/security/information/document112/ (дата обращения: 10.06.2023)

2. Термины МЧС России // Информационное противоборство // Министерство чрезвычайных ситуаций. URL: https://mchs.gov.ru/ministerstvo/o-ministerstve/terminy-mchs-rossii/term/888 (дата обращения: 10.06.2023)

3. Attention Is All You Need // Cornel University – 2017. (дата обращения 10.06.2023) URL: https://arxiv.org/abs/1706.03762 (дата обращения 10.06.2023)

4. Генеративные диалоговые модели: как мы разговорили виртуальных ассистентов Салют // Хабр Сообщество IT-специалистов – 2021. URL: https://habr.com/ru/companies/sberdevices/articles/589969/ (дата обращения 10.06.2023)

5. Build a Conversational Chatbot with Rasa Stack and Python – Rasa Core // Medium – 2019. URL: https://itsromiljain.medium.com/build-a-conversational-chatbot-with-rasa-stack-and-python-rasa-core-41b9c38c26b/ (дата обращения 10.06.2023)

6. Создай своего ИИ-ассистента с помощью ChatGPT и Streamlit // Хабр Сообщество IT-специалистов – 2023. URL: https://habr.com/ru/companies/ods/articles/729662/ (дата обращения 11.06.2023)

7. «Сабина Ai» – ИИ-аватар чатбота-психолога, с которым можно общаться как с человеком // vc.ru – 2022. URL: https://vc.ru/tribuna/518295-sabina-ai-ii-avatar-chatbota-psihologa-s-kotorym-mozhno-obshchatsya-kak-s-chelovekom/ (дата обращения 11.06.2023)

8. «Яндекс» добавил нейросеть YandexGPT (YaGPT) в виртуальный помощник «Алиса» // Хабр Сообщество IT-специалистов – 2023. URL: https://habr.com/ru/news/735696/ (дата обращения 11.06.2023)

9. Большие языковые модели как новый инструмент в научной работе // Хабр Сообщество IT-специалистов – 2023. URL: https://habr.com/ru/articles/726606/ (дата обращения 10.06.2023)

10. Модуль Re для регулярных выражений в Python // Python.ru. URL: https://pythonru.com/osnovy/modul-re-dlja-reguljarnyh-vyrazhenij-v-python (дата обращения 12.06.2023)

11. Документация vk_api // vk_api. URL: https://vk-api.readthedocs.io/en/latest/index.html (дата обращения 12.06.2023)

12. Libraries // OpenAI API. URL: https://platform.openai.com/docs/libraries (дата обращения 12.06.2023)

13. Neural conversational models: как научить нейронную сеть светской беседе. Лекция в Яндексе // Хабр Сообщество IT-специалистов – 2017. URL: https://habr.com/ru/companies/yandex/articles/333912/ (дата обращения 12.06.2023)

14. Alpaca: A Strong, Replicable Instruction-Following Model // Stanford University Human-Centered Artificial Intelligence. URL: https://crfm.stanford.edu/2023/03/13/alpaca.html (дата обращения 13.06.2023)

15. Что такое коэффициент скорости обучения и как он улучшает характеристики глубокого обучения? // Хабр Сообщество IT-специалистов – 2019. URL: https://habr.com/ru/articles/469931/ (дата обращения 13.06.2023)

16. Что такое эпохи в нейронных сетях // Самоучитель. URL: https://ritorika.com.ua/tekst/32/chto-takoe-jepohi-v-nejronnyh-setjah (дата обращения 13.06.2023)

17. LSTM – сети долгой краткосрочной памяти // Хабр Сообщество IT-специалистов – 2017. URL: https://habr.com/ru/companies/wunderfund/articles/331310/ (дата обращения 13.06.2023)

AUTOMATION OF GENERATION OF COMMENTS USING A NEURAL NETWORK «ChatGPT»

A.D. Baibakova, I.V. Podyukov, N.S. Sokolov, K.Y. Sukhikh, A.N. Rabchevsky
Perm State University

Abstract. The study proposed a method for automating the process of generating comments in natural language using «ChatGPT» in the social network «VKontakte». This approach makes it possible to create comments with different shades and content. The results of subsequent analytical studies have shown that this method can be used by cyber forces in information warfare.
Keywords: *information warfare, information operations; attribute detection, duplicates, frequency of publica-tions.*

КОМПЬЮТЕРНОЕ ПИРАТСТВО – ПРОБЛЕМА XXI ВЕКА. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ

Е.Д. Баклушин, А.В. Черников
Пермский государственный национальный исследовательский университет

Аннотация. В статье рассматривается актуальная проблема компьютерного пиратства и методы/средства защиты информации. Анализируются масштабы и последствия противоправных действий для глобальной экономики, существующие правовые и технологические меры борьбы с нелегальным распространением цифровых данных. Особое внимание уделяется ситуации в России после введения санкций и ухода ряда зарубежных компаний в области информационной безопасности. Исследуются современные технологические решения, такие как: DRM-защита, цифровые водяные знаки, блокчейн и искусственный интеллект. Предлагаются направления совершенствования систем защиты цифровой интеллектуальной собственности с учетом комплексного подхода, включающего правовые, экономические, технологические и просветительские меры.
Ключевые слова: *компьютерное пиратство, защита авторских прав, DRM, цифровые водяные знаки, блокчейн, искусственный интеллект, цифровая экономика.*

Компьютерное пиратство в эпоху всеобщей цифровизации общества представляет собой серьезную угрозу для развития инновационной экономики и творческих индустрий. Незаконное копирование и распространение программного обеспечения (ПО), мультимедийного контента и других цифровых объектов интеллектуальной собственности наносит значительный ущерб правообладателям и экономике в целом. Поэтому актуальность данной темы не вызывает сомнения и носит глобальный характер, затрагивающей глобальную экономику мира.

По оценкам экспертов, мировой ущерб от онлайн-пиратства составляет 71 млрд. долларов ежегодно. В России ситуация особенно критична, потому что более 60% организаций используют нелицензионное ПО, а объем рынка контрафактного ПО оценивается в 1.5 млрд. долларов. Рост цифрового пиратства в условиях санкций и ухода ряда зарубежных компаний с российского рынка привел к увеличению спроса на нелегальный цифровой контент. При этом существующие меры защиты информации показывают недостаточную эффективность, а отношение общества к проблеме остается неоднозначным.

Поэтому целью данного исследования становится анализ существующих подходов к защите цифровых данных от пиратства и разработки рекомендаций по совершенствованию механизмов защиты интеллектуальной

собственности с учетом современных технологических возможностей и социально-экономических реалий.

Обзор существующих методов и средств защиты информации

Основными направлениями изучения данной темы в научной литературе являются анализ масштабов и экономических последствий пиратства, правовые аспекты защиты, технологические методы защиты контента, социально-экономические аспекты проблемы и перспективные направления борьбы с пиратством.

По данным ВЦИОМ на 21 сентября 2023 года мнения россиян по вопросу необходимости защиты авторских прав составили: 41% выразили согласие с тем, что авторы фильмов, книг и других объектов интеллектуальной собственности должны быть надежно защищены законом от нелегального распространения их произведений. Почти такой же процент – 39% респондентов ответили, что после общественного представления интеллектуальные произведения становятся достоянием общественности и авторы не вправе запрещать пользователям обмениваться ими на безвозмездной основе. Не смогли точно ответить на данный вопрос 20% [1].

На сегодняшний день основные правовые нормы в вопросе авторского права регулируются в российском законодательстве УК РФ, статья 146 и КоАП РФ, статья 7.12. Также лицензия с конечным пользователем на использование программ для ЭВМ (EULA) является особым видом договора, поскольку законодательством прямо предусмотрена возможность его оформления в виде договора присоединения, условия которого излагаются на приобретаемом экземпляре таких программы или базы данных либо на упаковке этого экземпляра. Начало использования таких программы или базы данных конечным пользователем, как оно определяется этими стандартными условиями, означает его согласие на заключение лицензионного договора [2].

Из технических средств защиты и перспективных методов защиты информации можно рассматривать: **DRM-защита**, которая представляет собой набор технологий, используемых для контроля использования цифровых медиа данных и устройств. Эта технология позволяет правообладателям ограничивать способы, которыми их цифровой контент может быть использован, копирован или распространён покупателями. DRM может применяться к различным типам данных, включая музыку, фильмы, программное обеспечение и электронные книги. Принцип работы DRM обычно включает шифрование контента и требует от пользователя получения ключа для его дешифрования. Этот ключ связан с определёнными условиями использования, такими как количество устройств, на которых может быть воспроизведён контент, или срок, на который контент может быть доступен. При попытке доступа к контенту DRM-система проверяет, соответствуют ли условия использования политикам правообладателя, и разрешает или блокирует доступ. **Watermarking** или **водяные знаки** представляют собой метод внедрения невидимой или видимой информации в

цифровые данные (такие как изображения, видео, аудио) для защиты авторских прав, идентификации источника и предотвращения несанкционированного распространения. Эта технология играет ключевую роль в управлении цифровыми правами (DRM) и может использоваться для различных целей, включая подтверждение подлинности, отслеживание происхождения и доказательство владения. **Блокчейн** – это децентрализованная база данных, состоящая из связанных между собой блоков информации, которые защищены криптографическими методами. Блокчейн служит основой для цифровых денег, а также может использоваться в различных приложениях за пределами финансов, включая смарт-контракты, цепочки поставок, идентификацию и защиту интеллектуальной собственности. В 2024 году особое внимание уделяется использованию **НФТ (невзаимозаменяемых токенов**) для защиты авторских прав на цифровые произведения, обеспечивая каждому объекту уникальный цифровой сертификат. Новое применение получает и **искусственный интеллект (ИИ)** – для обнаружения и блокировки пиратского цифрового контента. Алгоритмы машинного обучения способны анализировать большие объемы данных в сети, выявляя и блокируя распространение копий цифрового контента без разрешения правообладателей. В 2024 году ИИ не только отслеживает нарушения, но и автоматически уведомляет об этом правообладателей, предоставляя подробные отчеты о найденных нарушениях [3][4].

Социально-экономические аспекты проблемы, включая причины распространения пиратства и влияние на различные отрасли экономики, рассматриваются в социологических и экономических исследованиях. За 2023 год российские геймеры скачали пиратские копии видеоигр на общую сумму свыше 324 млрд. руб. Об этом сообщили в пресс-службе онлайн-школы геймдева XYZ School. Общий уровень цифрового пиратства в конце 2023 года вырос на 4% и достиг отметки в 73% от общего числа геймеров. Пираты при отсутствии затрат на производство цифрового контента ежегодно зарабатывают около двух миллиардов долларов на рекламе и подписках. Их рентабельность достигает порядка 90 процентов, отмечают в Ассоциации кинематографистов, за счет более широкого выбора цифрового контента, чем у легальных платформ. Подписка на пиратские сервисы стоит от пяти до десяти долларов, в то время как у легальных площадок – около 20 долларов. Сейчас нелегальное распространение цифрового контента обходится экономике США примерно в 30 миллиардов долларов упущенной выгоды в год и примерно в 250 тысяч рабочих мест. Ущерб для мировой экономики оценивают в 71 миллиард долларов ежегодно. За 2023 год пользователи совершили 141 млрд. посещений сайтов с пиратским видеоконтентом по всему миру, а доходы пиратских сервисов в России за последние два года выросли на 71.4% и по итогам 2023 года составили 12 млрд. рублей, подсчитало агентство InterMedia в отчёте «Экономика культуры России». При этом оборот легальных онлайн-кинотеатров в 2022 году упал на 13%, с 99.6 млрд. рублей в 2021-м до 86.6 млрд. рублей в 2022-м, а в 2023 году прирос только на 3%, до 89.7 млрд. рублей [5][6][7].

В результате проведенных теоретических исследований различных источников можно отметить следующее, что проблема цифрового пиратства является многогранной и требует комплексного подхода к ее решению. Эффективная борьба с цифровым пиратством возможна только при сочетании правовых, технологических и социально-экономических мер.

Пути решения проблемы борьбы с цифровым пиратством

На основе проведенного выше анализа, можно сформулировать следующие ключевые задачи для решения проблем цифрового пиратства:

1. провести анализ современного состояния проблемы цифрового пиратства в России и мире, включая оценку масштабов распространения нелегального цифрового контента;

2. провести изучение экономических последствий пиратства для различных отраслей и анализ факторов, способствующих росту пиратства в условиях санкций;

3. исследовать существующие методы защиты от пиратства, включая правовые механизмы, технологические решения и экономические меры; оценить эффективность применяемых методов защиты и выявить их недостатки;

4. изучить новые перспективные технологии и подходы к защите интеллектуальной собственности, такие как применение искусственного интеллекта для обнаружения нарушений, использование блокчейна и NFT для защиты авторских прав, разработка платформ совместного использования дохода;

5. разработать комплекс рекомендаций по совершенствованию системы защиты от пиратства, включающий предложения по улучшению законодательной базы, рекомендации по внедрению новых технологических решений, меры по формированию культуры легального потребления контента и экономические стимулы для развития легального рынка цифрового контента;

6. оценить потенциальную эффективность предложенных мер и их влияние на снижение уровня пиратства в России. Решение этих задач позволит сформировать целостное представление о проблеме компьютерного пиратства и разработать эффективную стратегию борьбы с ним, учитывающую современные технологические возможности и социально-экономические реалии.

Решить все задачи, описанные выше в данной работе, не представляется возможным, поэтому далее будут описаны проблемы по каждой из задач и намечены пути решения. Более подробные пути решения задач будут описаны в других научных материалах.

Из существующих на сегодняшний день методах и средствах в России по борьбе с цифровым пиратством можно выделить частично работающие:

1. В России на сегодняшний день предусмотрена административная и уголовная ответственность за нарушение авторских прав, однако эффек-

тивность правоприменения остается низкой (см. информацию выше). Аналогично экономические меры, направленные на развитие легальных онлайн-сервисов и гибкую ценовую политику правообладателей, по эффективности существующих методов показывают, что, несмотря на наличие правовых и технологических мер защиты, уровень пиратства в России остается высоким. Это свидетельствует о недостаточной эффективности существующих методов и необходимости их совершенствования.

2. Применение новых технологий и подходов к защите интеллектуальной собственности включающих применение искусственного интеллекта для обнаружения и блокировки пиратского цифрового контента, использование блокчейна и NFT для защиты авторских прав, создание платформ совместного использования дохода также не позволяют полностью решить проблемы цифрового пиратства. Каждый из методов в той или иной степени снижает возможности нарушения авторских прав: ИИ-алгоритмы анализируют большие объемы данных в сети, выявляя и блокируя распространение нелегальных копий цифрового контента; блокчейн и NFT обеспечивают каждому объекту уникальный цифровой сертификат, что затрудняет незаконное копирование; цифровые платформы распространения цифрового контента совместного использования стимулируют легальное потребление контента, предоставляя его по подписке или за определённую плату с автоматическим распределением доходов между всеми участниками процесса.

Рекомендации

Из описанного выше материала можно сделать следующие выводы/рекомендации по совершенствованию системы защиты от цифрового пиратства включает:

1. улучшение законодательной базы,
2. внедрение новых технологических решений,
3. формирование культуры легального потребления и создание экономических стимулов.

В качестве примера конкретных рекомендаций можно предложить: ужесточить ответственность за нарушение авторских прав, упростить процедуру блокировки пиратских ресурсов, поддержать разработку и внедрение AI-систем для обнаружения нарушений, создать национальную блокчейн-платформу для регистрации авторских прав, проводить информационные кампании о вреде цифрового пиратства, развивать отечественные онлайн-платформы для распространения легального контента и ввести налоговые льготы для компаний, инвестирующих в защиту интеллектуальной собственности.

Потенциальная эффективность предложенных мер может оцениваться как высокая. По оценкам различных мировых экспертов, реализация подобных мер в других странах позволила снизить уровень пиратства на 4-5% ежегодно. При условии последовательной реализации предложенной

стратегии, можно ожидать снижения уровня пиратства в России до 40-50% в течение 5–7 лет.

Заключение

Проблема компьютерного пиратства в России и мире остается острой и требует комплексного подхода к ее решению. Проведенное исследование позволяет сделать вывод о том, что масштабы пиратства в России значительны и продолжают расти, особенно в условиях санкций и ухода ряда зарубежных компаний с рынка. Это наносит существенный ущерб экономике и препятствует развитию инновационных отраслей. Существующие методы защиты от пиратства, включая правовые механизмы и технологические решения, показывают недостаточную эффективность в современных условиях. Новые технологии, такие как искусственный интеллект, блокчейн и NFT, открывают новые возможности для защиты интеллектуальной собственности и требуют активного внедрения. Эффективная борьба с пиратством возможна только при комплексном подходе, сочетающем совершенствование законодательства, внедрение инновационных технологий защиты, развитие легальных сервисов и платформ, а также проведение просветительской работы среди населения. Необходимо не только ужесточать наказания за нарушения, но и создавать экономические стимулы для легального потребления контента, формировать культуру уважения к интеллектуальной собственности. Только объединив усилия государства, бизнеса и общества, можно добиться реального снижения уровня пиратства и обеспечить устойчивое развитие цифровой экономики в России.

Список литературы

1. Аналитический обзор: Онлайн-пиратство: за и против [Электронный ресурс] // ВЦИОМ. 2023. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/onlain-piratstvo-za-i-protiv (дата обращения: 18.04.2024).

2. Лицензионное соглашение с конечным пользователем EULA [Электронный ресурс] // IT-LEX. URL: http://www.it-lex.ru/licenzionnyj_dogovor/licenziya_konechnym_polzovatelem/ (дата обращения: 18.04.2024).

3. Российский рынок ПО: итоги 2023 года [Электронный ресурс] // Ассоциация предприятий компьютерных и информационных технологий (АПКИТ). 2024. URL: https://www.appp.ru/pr/news/3597/80433/ (дата обращения: 18.04.2024).

4. Methods to Protect Software From Piracy [Электронный ресурс] // Baeldung. URL: https://www.baeldung.com/cs/software-piracy-countermeasures (дата обращения: 18.04.2024).

5. В России в 2023 году спиратили игр на 324 млрд рублей [Электронный ресурс] // Ведомости. 2024. URL: https://www.vedomosti.ru/technology/articles/2024/02/01/1017829-v-rossii-v-2023-godu-spiratili-igr-na-324-mlrd-rublei (дата обращения: 18.04.2024).

6. В России за 2023 год спиратили игр на 324 миллиарда рублей [Электронный ресурс] // Playground.ru. 2023. URL: https://www.playground.ru/misc/news/za_2023_god_v_rossii_spiratili_igr_na_324_milliarda_rublej-1678016 (дата обращения: 18.04.2024).

7. Эксперты оценили ущерб от пиратства в России в 324 млрд рублей [Электронный ресурс] // Лента.ру. 2024. URL: https://lenta.ru/news/2024/01/24/piracy/ (дата обращения: 18.04.2024).

COMPUTER PIRACY – THE PROBLEM OF THE 21ST CENTURY. METHODS AND MEANS OF PROTECTION

E.D. Baklushin, A.V. Chernikov
Perm State University

Abstract. The article deals with the current problem of computer piracy and methods/means of information protection. It analyzes the scale and consequences of illegal actions for the global economy, existing legal and technological measures to combat illegal distribution of digital data. Special attention is paid to the situation in Russia after the imposition of sanctions and the departure of a number of foreign companies in the field of information security. Modern technological solutions such as: DRM-protection, digital watermarks, blockchain and artificial intelligence are studied. Directions for improving digital intellectual property protection systems are proposed, taking into account a comprehensive approach that includes legal, economic, technological and educational measures.

Keywords: *computer piracy, copyright protection, DRM, digital watermarks, blockchain, artificial intelligence, digital economy.*

СОВРЕМЕННЫЙ ПОДХОД К МОНИТОРИНГУ БЕЗОПАСНОСТИ КОНТЕЙНЕРНЫХ СРЕД

С.Г. Вьюгов, А.В. Козачок
Академия Федеральной службы охраны Российской Федерации

Аннотация. В статье рассматриваются вопросы мониторинга безопасности в реальном времени, которые становятся не просто дополнительной мерой, а ключевым элементом защиты. Рассматривается инструмент Falco для решения задачи мониторинга безопасности.
Ключевые слова: *мониторинг безопасности, контейнерные среды, защита контейнеров, Falco.*

Введение

В настоящее время информационные технологии развиваются с высокой скоростью. Создание микросервисной архитектуры, использование современных фреймворков и масштабируемых приложений требуют значительных вычислительных ресурсов. Однако в условиях высокой конкуренции и оптимизации затрат компаний возникла задача эффективного использования существующего вычислительного ресурса без ущерба производительности и отказоустойчивости. Для решения данных задач были созданы технологии виртуализации и контейнеризации, которые позволили рационально распределить ресурсы, а также адаптировать рабочую среду к изменениям в режиме реального времени.

Виртуализация – группа технологий, основанных на преобразовании формата и параметров программных и сетевых запросов к компьютерным ресурсам с целью обеспечения независимости процессов обработки информации от программной или аппаратной платформы информационной системы [1]. Главной составляющей этой технологии является виртуальная машина (ВМ), представляющая собой изолированную программную среду, которая эмулирует аппаратное окружение определенной платформы. В основе виртуальной вычислительной среды лежит гипервизор – программное средство распределения аппаратных ресурсов между виртуальными машинами. Технология виртуализации позволяет сократить затраты на физическое оборудование, повысить эффективность использования вычислительных ресурсов, обеспечить высокую устойчивость к сбоям и высокую надежность системы.

Контейнеризация – метод упаковки программного кода в единый исполняемы файл вместе с библиотеками и зависимостями. В результате создается контейнер – единый исполняемый файл, который стабильно работает на любой инфраструктуре. Технология контейнеризации предоставляет разработчикам возможность создания приложений, которые изначально адаптированы для работы в распределенных средах [2]. В отличие

от виртуализации, контейнеры используют общее ядро операционной системы, делая их легковесными, что значительно сокращает время запуска по сравнению с виртуальными машинами. Архитектура технологий виртуализации и контейнеризации представлены на рис. 1.

Рис. 1. Архитектура технологий контейнеризации и виртуализации

Контейнеры и виртуальные машины имеют схожее функциональное назначение, однако между ними существуют принципиальные различия. Виртуальные машины работают на основе собственного ядра операционной системы и обладают изолированными ресурсами. Контейнеры, напротив, используют общее ядро хостовой операционной системы, а их ресурсы не изолированы полностью. Технология контейнеризации применяется для:

1. построения архитектуры микросервисов;
2. создания сегментов баз данных;
3. автоматизации доставки приложений;
4. экономии места и памяти на устройствах;
5. повышения уровня безопасности системы;
6. увеличения скорости и эффективности работы системы.

Таким образом, технология контейнеризации больше подходит для построения микросервисных систем за счет своей архитектуры, а также позволяет эффективнее использовать имеющиеся вычислительные ресурсы.

Угрозы безопасности контейнеров

Контейнеризация, не смотря на ее удобство и эффективность, обладает более низким уровнем изоляции по сравнению с виртуализацией. Это создает новые сценарии угроз информационной безопасности, представленные на рисунке 2. Основные угрозы включают:

1. получение доступа из сети Интернет в контейнер;
2. получение доступа из одного контейнера в другой;
3. получение доступа к хостовой ОС из докера (побег);
4. получение доступа к мастер-узлу Kubernetes из докера;

5. получение доступа к API серверу из докера.

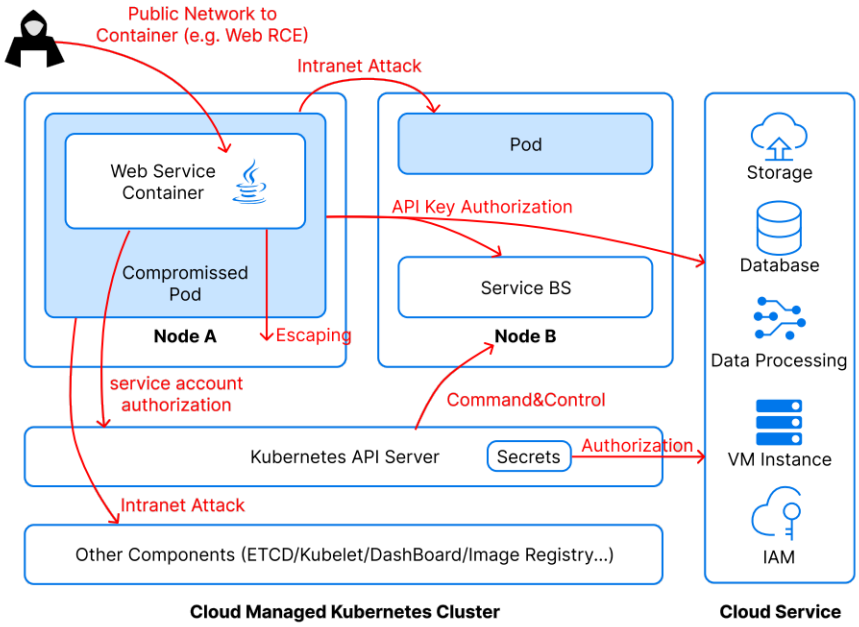

Рис. 2. Сценарии угроз информационной безопасности для технологии контейнеризации

Контейнер является короткоживущей сущностью, которая часто перезапускается, поэтому злоумышленнику достаточно тяжело в нем закрепиться, а хостовая операционная система перезапускается и модифицируется намного реже, следовательно, наиболее вероятный вектор угрозы – это совершение «побега» из докера в хостовую ОС. Целью злоумышленника при данном сценарии угрозы являются: возможность получения прав на остальные контейнеры, конфигурационные файлы, пароли, сертификаты и иная информация, распространение которой может нанести ущерб.

Классические контейнеры разделяют между собой ядро хостовой ОС, таким образом системные вызовы, которые идут из контейнера, проходят через хостовое ядро и если в нем присутствуют уязвимости, то возникает потенциальная возможность получения злоумышленником доступа к хостовой ОС. На данный момент известны следующие уязвимости для совершения «побега»:

1. CVE-2024-21626
2. CVE-2024-0132
3. CVE-2023-3389
4. CVE-2023-0461
5. CVE-2022-0847
6. CVE-2022-0492

Таким образом, контейнеризация значительно упрощает процессы разработки и развертывания приложений, однако ее использование сопряжено с дополнительными рисками информационной безопасности, для минимизации которых требуется внедрение различных механизмов защиты.

Механизмы защиты контейнеров

Для предотвращения угроз в контейнерной инфраструктуре недостаточно полагаться только на встроенные возможности контейнерных платформ. Эффективная защита требует внедрения дополнительных мер, которые усложняют запуск вредоносного кода, уменьшают поверхность атаки и обеспечивают изоляцию на всех уровнях. Эти подходы помогают минимизировать риски, но не исключают полностью возможность эксплуатации новых уязвимостей или ошибок конфигурации.

Современные контейнерные среды представляют собой сложную инфраструктуру, где безопасность должна обеспечиваться на всех уровнях изоляции. Применение таких механизмов защиты как Seccomp, AppArmor, SELinux, не исключает риск возникновения событий информационной безопасности. Современные угрозы, такие как «побег» из контейнера, несанкционированный доступ к хосту или утечка конфиденциальных данных, требуют применения инструментов мониторинга безопасности в реальном времени. Злоумышленники адаптируют свои атаки под облачные и контейнерные среды, действуя максимально быстро. Поэтому для оперативного выявления угроз системы безопасности должны не только регистрировать подозрительное поведение, но и генерировать уведомления в режиме реального времени, позволяя оперативно реагировать на потенциальные инциденты.

Одним из ведущих инструментов для мониторинга безопасности контейнеров является Falco. Это облачный инструмент с открытым исходным кодом, предназначенный для обеспечения безопасности в реальном времени на хостах, контейнерах, Kubernetes и облачных платформах. Falco анализирует события ядра Linux и другие данные, сравнивая их с заранее определенными или пользовательскими правилами. При выявлении подозрительного поведения инструмент генерирует уведомления, позволяя оперативно реагировать на инциденты [3].

Архитектура Falco состоит из трех основных компонентов (рисунок 3):

1. Falco Engine – основной компонент, отвечающий за мониторинг системных вызовов, сетевого трафика и других системных событий. Он использует механизм eBPF ядра Linux для захвата и анализа системных событий.

2. Правила Falco – заранее заданные правила, определяющие критерии для обнаружения аномалий и угроз. Правила можно настроить в соответствии с конкретными требованиями безопасности, они записываются в формате YAML.

3. Выходные данные – этот компонент обрабатывает выходные данные Falco Engine, предоставляя оповещения и уведомления при срабатывании правила.

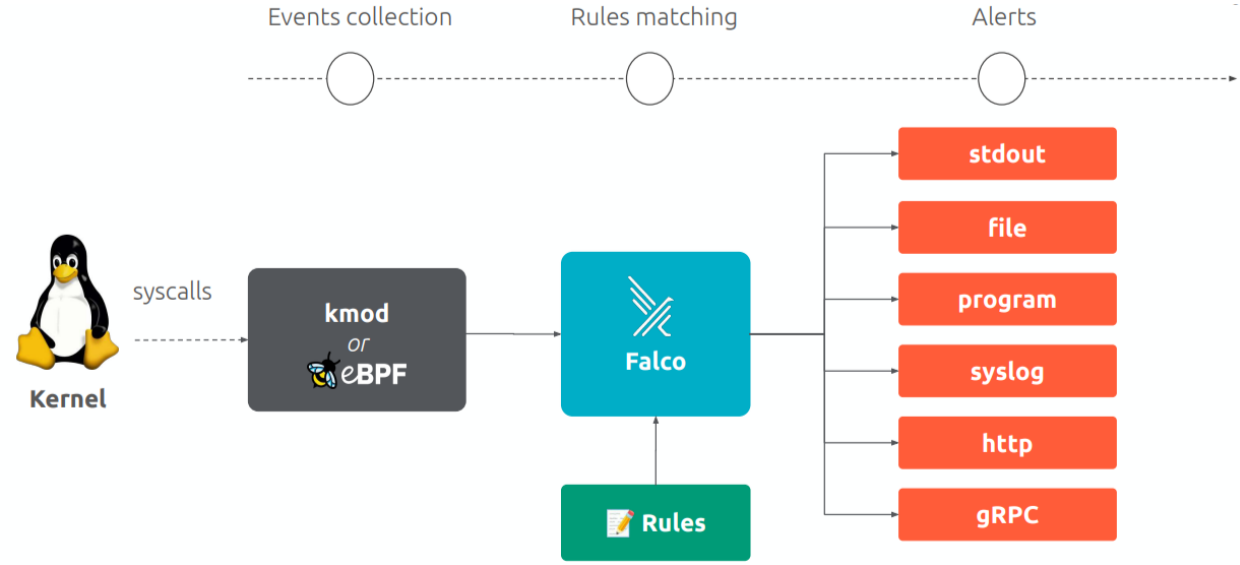

Рис. 3. Архитектура инструмента мониторинга системных вызовов Falco

Falco использует мощный механизм правил для анализа системных вызовов и обнаружения подозрительных событий. Каждое правило описывает определенное условие (condition), при котором действие или событие считается аномальным или потенциально опасным. Если событие соответствует условию, Falco генерирует оповещение (alert) для уведомления администратора системы [4]. Пример правила представлен на рисунке 4.

```
rule: shell_in_container
desc: notice shell activity within a container
condition: >
  evt.type = execve and
  evt.dir = < and
  container.id != host and
  (proc.name = bash or
   proc.name = ksh)
output: >
  shell in a container
  (user=%user.name container_id=%container.id container_name
  shell=%proc.name parent=%proc.pname cmdline=%proc.cmdline)
priority: WARNING
```

Рис.4. Правило Falco для мониторинга активности оболочки внутри контейнера

Когда Falco обнаруживает событие, соответствующее условию правила, оно немедленно создает оповещение, которое может быть отправлено по различным каналам, таким как:

1. логи системы (syslog);
2. интеграции с DevOps-инструментами (Slack, PagerDuty);
3. инструменты SIEM для централизованного управления безопасностью;
4. webhook для автоматизации ответа на инциденты.

Заключение

Современные контейнерные среды предоставляют организациям большие возможности для масштабируемости, гибкости и ускорения процессов разработки и развертывания приложений. Однако их тесная интеграция с хостовой ОС создают уникальные угрозы в области информационной безопасности. В таких условиях мониторинг безопасности в реальном времени становится не просто дополнительной мерой, а ключевым элементом защиты. Использование инструментов, таких как **Falco**, позволяет не только обнаруживать подозрительное поведение и предотвращать инциденты, но и обеспечивать соответствие политик безопасности требованиям современных DevSecOps процессов. Гибкость настройки, возможность адаптации правил и интеграции с DevOps процессами делают Falco и его аналоги незаменимыми инструментами для построения многоуровневой защиты.

Список литературы

1. ГОСТ Р 56938-2016. Информационная технология. Методы и средства защиты информации. Средства виртуализации. Общие технические требования и методы испытаний. – Введ. 2017-01-01. – М.: Стандартинформ, 2016. – 27 с.

2. Gantikow, H., Reich, C., Knahl, M., Clarke, N. Rule-based Security Monitoring of Containerized Workloads // Proceedings of the 9th International Conference on Cloud Computing and Services Science (CLOSER 2019), pp. 543–550. DOI: 10.5220/0007770005430550. Lisbon: SCITEPRESS, 2019. ISBN: 978-989-758-365-0. DOI: 10.5220/0007770005430550.Lisbon

3. Wong, A. Y., Chekole, E. G., Ochoa, M., & Zhou, J. (2023). On the Security of Containers: Threat Modeling, Attack Analysis, and Mitigation Strategies. Computers & Security. Preprint submitted February 19, 2023. Singapore University of Technology and Design, ETH Zurich. DOI: 10.1016/j.cose.2023.103140 EDN: HPKFGD

4. Falco: Open Source Runtime Security. [Электронный ресурс]. – URL: https://falco.org/ (дата обращения: 24.11.2024).

MODERN APPROACH TO MONITORING THE SAFETY OF CONTAINERIZED ENVIRONMENTS

S.G. Vyugov, A.V. Kozachok
Academy of the Federal Guard Service of the Russian Federation

Abstract. The article deals with the issues of real-time security monitoring, which become not just an additional measure, but a key element of protection. Falco tool for solving the problem of security monitoring is considered.
Keywords: *security monitoring, container environments, container protection, Falco.*

ЭВОЛЮЦИЯ МЕТОДОЛОГИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ОБОСТРЕНИЯ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

А.Н. Зотов, А.А. Некрасов
Пермский военный институт войск национальной гвардии РФ

Аннотация. В данной работе исследуется эволюция методологии информационной безопасности в условиях обострения информационного противоборства, включая «гибридные войны». Анализируются ключевые этапы развития информационной безопасности, от традиционных подходов к защите данных до современных концепций, учитывающих информационно-психологические и когнитивные аспекты безопасности. Особое внимание уделяется влиянию новых технологий и форм информационных войн на трансформацию методологии информационной безопасности и формирование новых подходов к защите национального суверенитета в информационном пространстве.
Ключевые слова: *информационная безопасность, информационное противоборство, кибербезопасность, информационно-психологическая безопасность, когнитивная безопасность, национальный суверенитет, информационные войны.*

Современный мир характеризуется беспрецедентной зависимостью от информационных и коммуникационных технологий, что одновременно расширяет возможности и увеличивает риски. Усиление информационного противоборства, проявляющееся в различных формах – от киберпреступности до целенаправленных информационных кампаний и «гибридных войн», – требует кардинальной переоценки традиционных подходов к информационной безопасности. Методология информационной безопасности эволюционирует от узкоспециализированной защиты данных к комплексной системе, учитывающей политические, экономические, социальные и психологические факторы.

Методология информационной безопасности находится в постоянном развитии. Новые технологии, новые формы информационного противоборства и возрастающая сложность киберугроз требуют постоянной адаптации и поиска новых решений. Будущее методологии связано с развитием искусственного интеллекта, использованием больших данных для анализа угроз, совершенствованием методов защиты критическо-важной инфраструктуры и усилением международного сотрудничества в борьбе с трансграничной киберпреступностью. Комплексный и проактивный подход, акцент на подготовке высококвалифицированных кадров и постоянное совершенствование нормативно-правовой базы остаются ключевыми

факторами обеспечения национальной информационной безопасности в условиях растущего информационного противоборства.

На начальных этапах развития информационной безопасности доминировала концепция CIA-триады (Confidentiality, Integrity, Availability – конфиденциальность, целостность, доступность). Этот подход фокусировался на технических аспектах защиты данных – криптографии, контроле доступа, резервном копировании и других мерах, направленных на предотвращение несанкционированного доступа, модификации или уничтожения информации. Однако быстро меняющийся технологии способствовали появлению новых форм угроз, продемонстрировали ограничения данного подхода. Традиционные методы оказались неэффективными против сложных, многовекторных атак, использующих социальную инженерию, дезинформацию и другие методы.

Появление интернета, глобальных и социальных сетей привело к появлению новых видов угроз для безопасности и целостности государства и общества. Первая из которых является киберпреступность. К ней относится широкий спектр преступных деяний, от фишинга и кражи персональных данных и финансовых средств, до вредоносных программ и атак на особо важные части инфраструктуры. Государственно-спонсируемый хакинг, это целенаправленные атаки на государственные органы, компании и частные лица, осуществляемые с целью шпионажа, саботажа или дестабилизации положения в стране или организации. Информационные войны, включают использование информационных технологий для достижения политических, экономических или военных целей, включая дезинформацию, пропаганду, манипуляцию общественным мнением и создание хаоса. Гибридные войны, особый вид комбинации традиционных и нетрадиционных методов ведения войны, включая кибератаки, информационные кампании и дестабилизирующие действия. Информационно-психологическое воздействие, или же целенаправленное воздействие на психику населения страны и когнитивные процессы в обществе с целью дезориентации, подавления воли и манипулирования поведением. Все эти вызовы привели к необходимости переосмысления методологии информационной безопасности.

По причине быстроразвивающегося технического прогресса новое поколение развивается и взрослеет гораздо быстрее чем предыдущее. Они с раннего возраста имеют открытый доступ в интернет-пространство, имея возможность получать не цензурированный контент, в том числе из-за недостаточного получения информации от своих родителей и слабого контроля. Важно заметит, что молодое поколение отличается высокими познаниями в области информационной безопасности, но в силу возраста и высокого желания проявления себя социуму, информационно-психологическое воздействие имеет по отношению к ним максимально сильный характер. Таким образом они становятся основными объектам воздействия. Учитывая эти факты, можно предположить, что формирование будущей методологии информационной безопасности в том числе основывается именно на них.

Также, из-за обострения информационного противоборства и осложнения обстановки на мировой арене, проявляющееся в виде новых способах ведения боевых действий и пропаганды, методология учитывает политические, социально-демографические, экономические и психологические факты.

В настоящий момент современная методология информационной безопасности заключается:

В определении всех ценных информационных активов, такие как данные, системы и приложения. Выявление потенциально слабых мест в системах и процессах, которые могут быть использованы злоумышленниками. Определение потенциальных угроз, которые могут нанести ущерб информационным активам. Оценки вероятности возникновения каждой угрозы и потенциальных последствий для определения уровня риска каждого актива. Важна разработка и внедрение четких политик и процедур в области информационной безопасности, охватывающие все аспекты защиты информации. Использование различных технических средств защиты информации, таких как антивирусное программное обеспечение, брандмауеры, системы обнаружения вторжения и системы шифрования. Актуально внедрение административных мер, к примеру управление доступом, контроль изменений, а также качественное и своевременное обучение специалистов и пользователей. Не мало важно обеспечивать и физическую безопасность информационных систем и данных, включая контроль доступа к помещениям такого рода и защиту их от стихийных бедствий.

Постоянный мониторинг системы безопасности для выявления потенциальных угроз и инцидентов, так же разработка и внедрении планов реагирования на них. И в точном анализ произошедших инцидентов для выявления подобных ситуаций в будущем.

Эффективная информационная безопасность требует сильной правовой базы и международного сотрудничества. Государства разрабатывают и принимают законы и нормативные акты, регулирующие деятельность в сфере информационно коммуникационных технологий, предусматривающие ответственность за киберпреступления.

Не мало важен и регулярный аудит системы безопасности для оценки ее эффективности и выявления слабых областей, для дальнейшего улучшения. Частое обновление политики и процедур с учетом изменения в технологиях и угрозах.

Но самым главным является тот факт, что для эффективной работы и поддержания процесса саморазвития методологии, должна быть созданна ответственный за это искусственный интеллект, который поможет минимизировать риски и обеспечивать системы в круглосуточном порядке.

Наиболее эффективной политикой и методологией информационной безопасности, а также самой масштабной системы цензуры в мире, в настоящее время, обладает Китай. В стране организована так называемая система «Золотой щит» или же «Великий китайский файрвол». Она представляет собой firewall созданный с целью поддержания порядка в интернете и контроля деятельности пользователей для пресечения нежелатель-

ных для государства действий. Однако он обладает своими недостатками, одним из которых является большое ограничение в плане источников предоставляемой информации.

Современная методология информационной безопасности является наиважнейшим фактором существования любого государства, она должна представлять из себя комплексный, проактивный и адаптивный подход, направленный на минимизацию рисков и обеспечение безопасности информационных активов в динамично меняющейся среде.

Список литературы

1. Джура, Г. С. Информационно-психологическая безопасность личности в современных реалиях / Г. С. Джура // Вестник Донецкого национального университета. Серия Д: Филология и психология. – 2022. – № 3. С. 119-122. URL: https://www.elibrary.ru/download/elibrary_53876141_58059365.pdf. EDN: TZUVUY

2. Морозов, А. В. Психология информационной провокации / А. В. Морозов // Казанский педагогический журнал. – 2017. – № 6(125). – С. 27-35. URL: https://www.elibrary.ru/download/elibrary_30611528_51412637.pdf. EDN: ZTWRGP

3. Манойло, А. В. Информационные войны / А. В. Манойло // Геополитический журнал. – 2017. – № 5-6(20). – С. 28-36. URL: https://www.elibrary.ru/download/elibrary_32751839_91412484.pdf. EDN: YVAZFA

4. Сулейманова Ш.С., Назарова Е.А., Информационные войны: история и современность: Учебное пособие. – М.: Международный издательский центр «Этносоциум», 2017. 124 с. URL: https://mgimo.ru/upload/iblock/486/%D0%A1%D1%83%D0%BB%9E%D0%9D%D0%90%AB%D0%95%20%D0%92%D0%9E%D0%99%D0%9D%D0%AB. Pdf

5. Федорова, О. Н. Информационно-психологическая безопасность личности в информационном обществе / О. Н. Федорова // Вестник Дальневосточного государственного технического университета. – 2011. – № 2(7). – С. 21-34. URL: https://www.elibrary.ru/download/elibrary_22541053_37046639.pdf. EDN: SZGXNT

6. Ряжапов, Н. Х. Национальные интересы России в информационной сфере в условиях мировой нестабильности и меры их обеспечения / Н. Х. Ряжапов // Развитие науки и образования в условиях мировой нестабильности: современные парадигмы, проблемы, пути решения: Материалы Международной научно-практической конференции. В 2-х частях, Ростов-на-Дону, 29 октября 2021 года. Том Часть 1. – Ростов-на-Дону: ООО «Издательство ВВМ», 2021. – С. 101-110. URL: https://www.elibrary.ru/download/elibrary_47231698_67351052.pdf. EDN: ESSRPG

EVALUTION OF INFORMATION METODOLOGY SECURITY IN CONDITIONS OF AGGERESSIONAL INFORMATION CONFRONTATION

A.N. Zotov, A.A. Nekrasov
Perm Military Institute of the National Guard Troops of Russian Federation

Abstract. This paper examines the evolution of information security, methodology in the context of escalating, information confrontation, including «mental wars». Key stages of information security development are analyzed, from traditional approaches to data protection to modern concepts that take into account information-psychological and cognitive aspects of security. Particular attention is paid to the influence of new technologies and forms of information warfare on the transformation of the threatening methodology of information security and the formation of new approaches to protecting national sovereignty in the information space.
Keywords: *information security, information confrontation, cybersecurity, security, information-cognitive security, national sovereignty, information wars.*

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЛИНЕЙНЫХ И НЕЛИНЕЙНЫХ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ МАКСИМАЛЬНОЙ ДЛИНЫ ПРИ ПРИМЕНЕНИИ ИХ В ШИРОКОПОЛОСНЫХ СИСТЕМАХ СВЯЗИ С ПОВЫШЕННЫМИ ТРЕБОВАНИЯМИ К ИМИТОСТОЙКОСТИ

А.Л. Лобков
Пермский государственный национальный исследовательский университет

Аннотация. Рассматриваются вопросы, связанные с использованием линейных и нелинейных псевдослучайных последовательностей (ПСП) максимальной длины в широкополосных системах связи. Проводится сравнение методов их формирования, а также общее число получаемых линейных и нелинейных ПСП максимальной длины в зависимости от разрядности регистров сдвига. Анализируются их автокорреляционные функции (АКФ), эквивалентная линейная сложность. Делается вывод о возможном применении нелинейных ПСП в широкополосных системах связи, при возможном их преобразовании в ПСП с характеристиками АКФ, как и у линейных ПСП максимальной длины.
Ключевые слова: *псевдослучайные последовательности (ПСП), автокорреляционная функция (АКФ), эквивалентная линейная сложность (ЭЛС), регистр сдвига (РС).*

Проведем сравнительный анализ образования линейных и нелинейных псевдослучайных последовательностей (ПСП) максимальной длины, с использованием переключательных схем на основе регистров сдвига (РС).

Рассматривая образование линейных ПСП, можно отметить следующее: линейные ПСП максимальной длины (в частности *M*-последовательности) формируются с помощью линейных переключательных схем на основе РС (рис.1), где применяется регистр с k разрядами и в ПСП используется p различных видов импульсов (отличающихся фазами) выражаемых через следующее соотношение

$$N = p^k - 1, \qquad (1)$$

где: p – число различных используемых символов;

N – число импульсов в периоде ПСП.

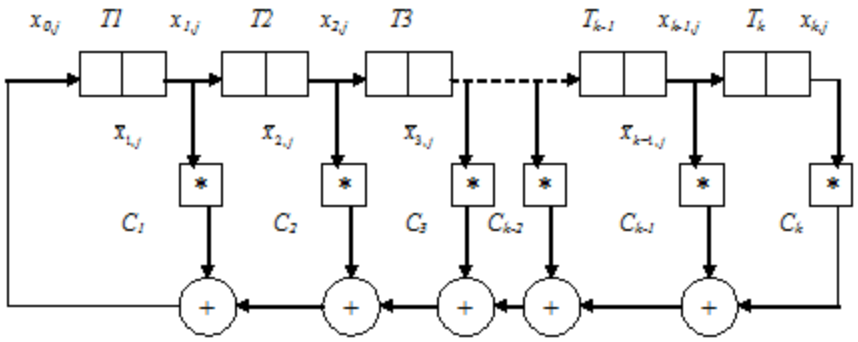

Рис. 1. Схема формирования линейных ПСП максимальной длины

Линейные ПСП максимальной длины обладают следующими свойствами:

1) единиц в ПСП на одну больше чем нулей;

2) можно легко подсчитать распределение длин серий из «нулей» и «единиц», которые одинаковы для одного и того же кода. Относительное положение этих серий меняется от последовательности, к последовательности, но число серий одинаковой длины остается без изменения;

3) функция автокорреляции (АКФ) кода максимальной длины такова, что для всех значений задержки она равна – единице, за исключением области 0 ± 1, где значения функции автокорреляции меняются от – 1 до

$2^n - 1$ (длина ПСП);

4) сложение по модулю 2 любой ПСП максимальной длины, с последовательностью, полученной любого циклического сдвига этой же последовательности, приведет к новой ПСП, которая представляет циклический сдвиг той же самой последовательности на другое число позиций;

5) каждое возможное состояние, или n – разрядная комбинация данного n – разрядного генератора, за время формирования полного периода кода, возникает в некоторый момент времени только один раз;

6) среди всех возможных комбинаций в РС, комбинация из k нулей (000…0) является запрещенной. Если в РС, по каким – либо причинам такая комбинация возникает, то колебания в РС сорвутся и РС установится в нулевое состояние.

Все вышеперечисленные свойства позволяют использовать линейные ПСП максимальной длины в широкополосных системах связи. Но данный вид ПСП не в полном объеме соответствует требованиям в построении сигнального обеспечения в имитостойких системах связи.

Для формирования нелинейных ПСП можно воспользоваться аналогичной схемой (рис.1) формирования линейных ПСП, добавив в нее схему совпадений **И** (рис.2).

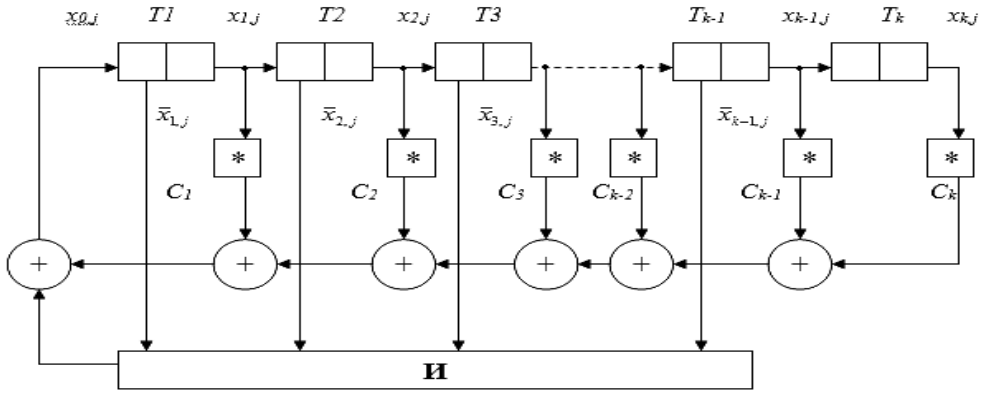

Рис. 2. Схема формирования нелинейных ПСП максимальной длины

Используя дополнительные логические операции, можно построить, таким образом, схему РС, в которой кодовая комбинация символов из k нулей перестает быть запрещенной. В этом случае период ПСП будет равен $N = p^k$, а получаемая в РС последовательность символов описывается нелинейным рекуррентным уравнением.

Рассмотрим принцип образования нелинейного рекуррентного уравнения. В схеме на рис.2, схема **И** является схемой совпадений $k-1$ единиц, то есть на выходе схемы **И** символ -1 появляется тогда, когда на всех схемах ее входа единицы. При этом:

$$\bar{x}_{l,j} = x_{l,j} + 1 (\mathrm{mod}\ p). \qquad (2)$$

Схема **И** на работу РС не влияет, за тем лишь исключением, что между кодовыми комбинациями 000…01 и 100…00 она создает комбинацию символов k нулей (000…00). Поэтому выбор характеристического многочлена (определение коэффициентов $C_1, \ldots, C_k$) для определения структуры РС, приведенного на рис.2, следует делать, так же как и для линейных ПСП.

Прямой символ на выходе l – го триггера на $j+1$ выражается через следующее соотношение

$$x_{0,j} = \sum_{l=1}^{k} c_l x_{l,j} + \prod_{l=1}^{k-1} \bar{x}_{l,j}, \qquad (3)$$

где: $\prod_{l=1}^{k-1} \bar{x}_{l,j} \equiv \begin{cases} 1 при \bar{x}_{l,j} = 1, \\ 0 при \bar{x}_{l,j} \neq 1 \end{cases}$ – операция символического умножения, выполняемого схемой **И**.

Используя формулу (2) нелинейное рекуррентное отношение (3) можно записать как

$$x_{0,j} = \sum_{l=1}^{k} c_l x_{l,j} + \prod_{l=1}^{k-1} (x_{l,j} + 1). \qquad (4)$$

Исходя из полученного рекуррентного уравнения формулу для расчета нелинейных ПСП возможных при данной разрядности РС k можно представить как

$$Q = 2^{2^{k-1}-k}, \qquad (5)$$

где: Q – получаемое количество нелинейных ПСП.

Сравним количество получаемых линейных и нелинейных ПСП в зависимости от разрядности РС используя формулы (1) и (5). Результат сравнения сведем в талб.

Таблица

Число разрядов регистра сдвига k	3	4	5	6
Количество линейных ПСП Q_M	2	3	6	6
Количество нелинейных ПСП $Q_{НРП}$	2	16	2048	67108864

Расчеты, представленные в табл. 1 показывают, что при разрядности РС $k > 4$ число нелинейных ПСП существенно выше числа линейных ПСП. Такое большое различие по числу ПСП объясняется тем, что введение нелинейных логических операций значительно расширяет возможности при проектировании формирующих схем.

Кроме рассмотренного выше способа формирования нелинейных ПСП, проводились исследования по построению:

1) схем РС линейной обратной связи с нелинейной внешней логикой (рис.3)

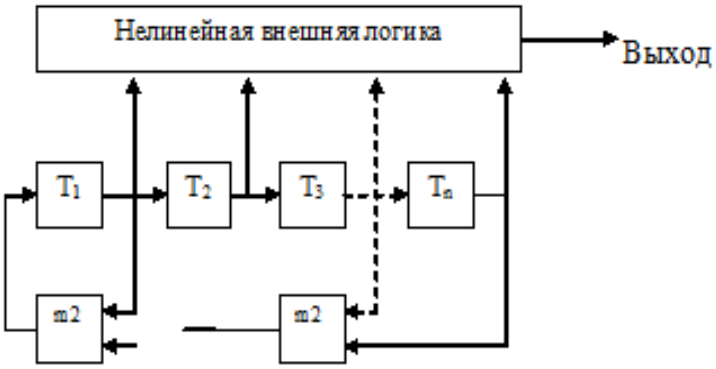

Рис. 3. Схема РСЛОС с нелинейной внешней логикой

2) схем формирования нелинейных ПСП из 3-х М – последовательностей, с реализацией алгоритма Джеффа (рис.4)

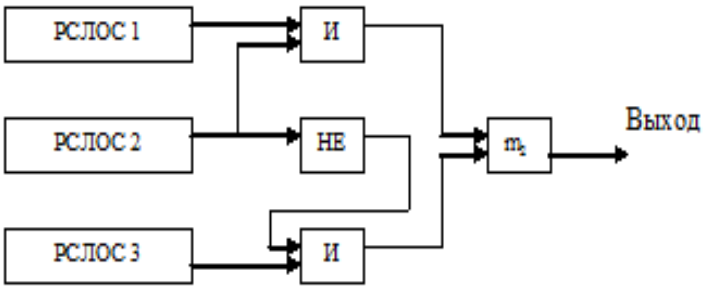

Рис. 4. Схема формирования нелинейной ПСП из трех М – последовательностей

Но рассмотренный выше способы формирования нелинейных последовательностей (как и другие изученные способы формирования нелинейных ПСП) обладает рядом существенных недостатков. В частности, в отличие от М – последовательности сумма двух сдвинутых нелинейных последовательностей не является циклически сдвинутой относительно исходной нелинейной последовательностью. Малый уровень боковых пиков (-1/N) периодической АКФ М – последовательностей является следствием того, что сумма двух М – последовательностей также является М – последовательностью. Так как нелинейные последовательности этим свойством не обладают, то можно предположить, что уровень боковых пиков их АКФ будет больше уровня боковых пиков АКФ М – последовательностей, что в конечном итоге приводит к возникновению флуктуационных шумов, не позволяющих их использовать в широкополосных системах связи с повышенными требованиями к имитостойкости.

Из всех изученных раннее способов формирования нелинейных ПСП максимальной длины наибольший интерес представляют нелинейные ПСП де Брейна.

Нелинейные рекуррентные ПСП, называемые последовательностями де Брейна или последовательными циклами, характеризуются тем, что каждое n – е состояние РС встречается на периоде ПСП один раз. Диаграмму состояний РС с нелинейной обратной связью можно представить

как граф де Брейна, в котором узлами являются переходы из ионного состояния РС $X = x_0, x_1, \dots, x_{n-1}$ в другое $Y = x_1, x_2, \dots, x_n$ (рис.5).

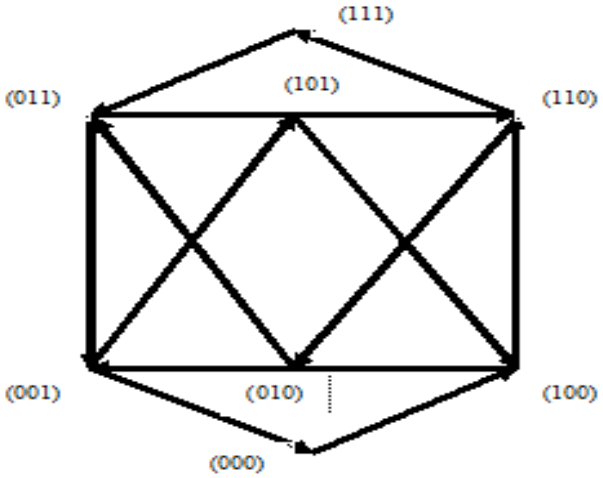

Рис. 5. Граф де Брейна для n = 3

Число нелинейных ПСП де Брейна длиной $L = 2^n$, возможных при данном n, также можно выразить через формулу (5)

$$Q = 2^{2^{n-1}-n}. \qquad (6)$$

Нелинейные ПСП де Брейна отличаются от линейных ПСП не только большим ансамблем и максимально возможным периодом, но и тем, что они сбалансированы по числу единиц и нулей и имеют высокую непредсказуемость в силу большой эквивалентной линейной сложности (C_s). Для этих ПСП C_s находится в пределах $2^{n-1} + n \le C_s \le 2^n - 1$, причем половина всех ПСП де Брейна имеет сложность $C_s \le 2^n - 1$. Также характерной особенностью ПСП де Брейна является то, что каждое n-ичное состояние РС встречается на периоде ПСП только один раз, что так же отражает построенный граф де Брейна для $n = 3$ (рис.5). Степенью ПСП де Брейна называется n наименьшее целое число, такое, что все n-ичные состояния $S = a_i, a_{i+1}, \dots, a_{i+n-1}$ являются разными на периоде последовательности.

ПСП де Брейна вызывают большой интерес при их возможном использовании в широкополосных системах связи не только тем, что они в максимальной степени приближаются к случайным последовательностям, но и тем, что они имеют хорошую статистику (нормальное распределение серий в последовательности), сбалансированных по числу нулей в периоде.

В настоящий момент времени не в полном объеме отработан алгоритм генерирования РС всего ансамбля нелинейных ПСП де Брейна для произвольных значений n.

Существуют алгоритмы нахождения функций обратной связи РС, генерирующих нелинейные ПСП де Брейна, основанные на объединении ко-

ротких циклов, имеющих длину $l<2^n$, в полный цикл длиной 2^n. Наиболее изучены методы объединения циклов, вырабатываемых суммирующим РС (рис. 6).

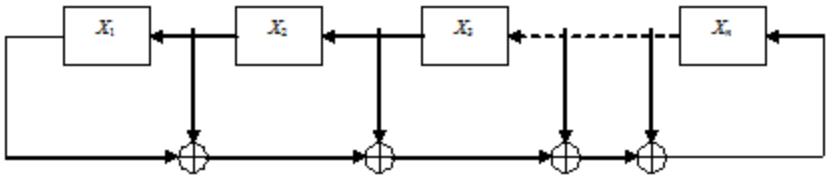

Рис. 6. Структурная схема простого суммирующего РС

Этот регистр имеет функцию обратной связи $f_c(x_1, x_2, x_3, \dots, x_n) = x_1 \oplus x_2 \oplus x_3 \oplus \dots \oplus x_n$. Набор циклов, генерируемых этими РС, задается сменой начального состояния РС. Объединение циклов производится по следующему алгоритму:

1) формируют k циклов простого РС сменой его начального состояния; составляют таблицы истинности для каждого начального состояния;

2) отыскивают смежные циклы, которые содержат сопряженные $(x_1, x_2, \dots, x_{n-1}, 0)$ и $(x_1, x_2, \dots, x_{n-1}, 1)$ или парные $(0, x_2, \dots, x_n)$ и $(1, x_2, \dots, x_n)$ состояния;

3) по парным объединением смежных циклов путем взаимной замены сопряженных (или парных) состояний получают полный цикл.

Полный цикл, основанный на объединении циклов суммирующего РС, можно выразить через оцениваемое значение $\approx 2^{n^2/4}$ или более точно $\prod_{k=1}^{[\frac{n-2}{2}]} \binom{n-1}{2k}$ полных циклов.

Рассмотренный метод генерирования нелинейных ПСП де Брейна позволяет использовать их в тех случаях, когда не предъявляются высокие требования к корреляционным свойствам ПСП. Но использовать их для построения сигнального обеспечения в широкополосных системах связи с повышенными требованиями к имитостойкости так же невозможно, как и другие виды нелинейных ПСП, так как уровень боковых пиков АКФ нелинейных ПСП де Брейна (рис.7) так же будет больше уровней боковых пиков АКФ М – последовательностей (рис.8).

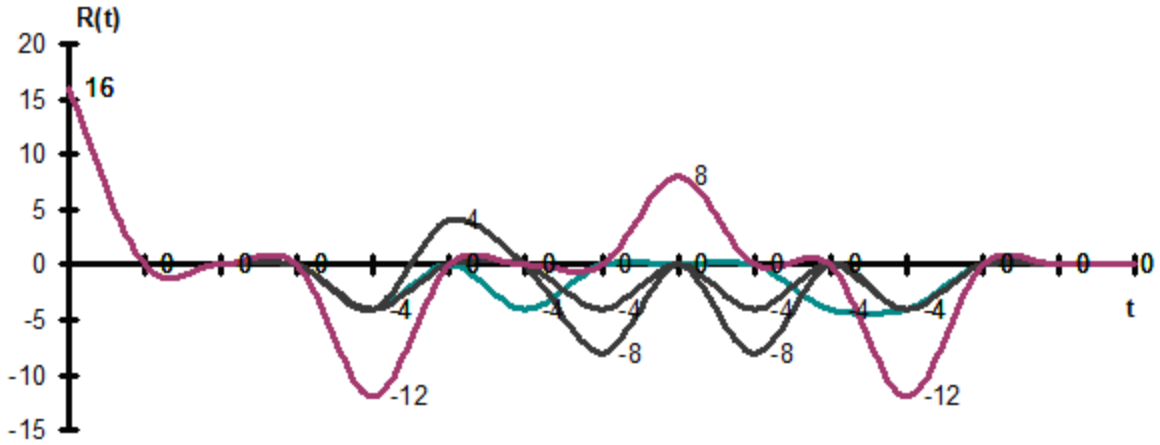

Рис. 7. График полного ансамбля АКФ нелинейных ПСП де Брейна при разрядности РС n=4

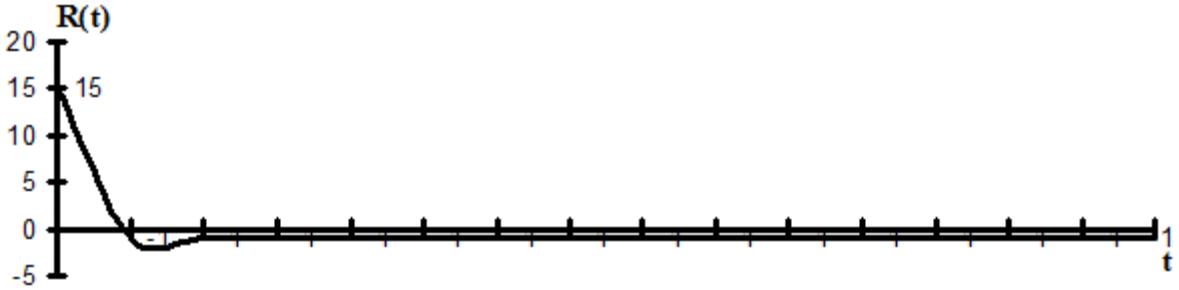

Рис. 8. График полного ансамбля АКФ линейных М-последовательностей при разрядности РС n=4

Для возможного применения нелинейных ПСП де Брейна в широкополосных системах связи с повышенными требованиями к имитостойкости необходимо:

1) разработать правила формирования выбора обратных связей РС для формирования нелинейных ПСП де Брейна максимальной длины;

2) провести сравнение полученных нелинейных ПСП де Брейна максимальной длины с линейными ПСП максимальной длины, например, ПСП Уолша.

3) провести исследование АКФ нелинейных ПСП де Брейна с учетом формирования полных кодовых словарей;

При полученных положительных результатах можно предположить, что нелинейные ПСП де Брейна возможно будет использовать в широкополосных системах связи с повышенными требованиями к имитостойкости.

Список литературы

1. Беляев В.С. Шумоподобный фазоманипулированный сигнал на основе нелинейной псевдослучайной последовательности и согласованный фильтр для его обработки. Радиотехника №9 1991 г.

2. Варакин Л.Е. Системы связи с ШПС. – М. Радио и связь 1985 г.

3. Голубев Б.И., Ефимов А.В., Скворцов В.А. Ряды и преобразования Уолша: Теория их применения. М. Наука 1987 г.

4. Диксон Р.К. Широкополосные системы. М. Связь 1979 г.
5. Ипатов В.П., Камалетдинов Б.Ж., Самойлов И.М. Исследования корреляционных свойств М – последовательностей и ансамблей. Радиотехника и электроника т. 34 №2, 1989 г.
6. Кругликов Н.В., Крейнделин В.Б. Ансамбль нелинейных псевдослучайных последовательностей с хорошими корреляционными свойствами. Радиотехника №8 1994 г.
7. А.А. Ожиганов, И.Д. Захаров. Применение последовательностей де Брейна для построения псевдорегулярных кодовых шкал. Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики. Научно-технический вестник информационных технологий, механики и оптики 2012 г., № 2 (78).

COMPARATIVE ANALYSIS OF LINEAR AND NONLINEAR PSEUDORANDOM SEQUENCES OF MAXIMUM LENGTH WHEN USED IN BROADBAND COMMUNICATION SYSTEMS WITH INCREASED REQUIREMENTS FOR IMAGE STABILITY

A.L. Lobkov
Perm State University

Abstract. The issues related to the use of linear and nonlinear pseudorandom sequences (PSPs) of maximum length in broadband communication systems are considered. The methods of their formation are compared, as well as the total number of linear and nonlinear maximum length PSPs obtained, depending on the bit depth of the shift registers. Their autocorrelation functions (ACF) and equivalent linear complexity are analyzed. The conclusion is made about the possible use of nonlinear PSPs in broadband communication systems, with their possible transformation into PSPs with ACF characteristics, as in linear PSPs of maximum length.
Keywords: *pseudorandom sequences (PSP), autocorrelation function (ACF), equivalent linear complexity (ELS), shift register (RS).*

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЕ ВОЗДЕЙСТВИЕ НА ЧЕЛОВЕКА В СОВРЕМЕННОМ ОБЩЕСТВЕ

Д.С. Маликов, А.А. Некрасов
Пермский военный институт войск национальной гвардии РФ

Аннотация. В данной работе рассматривается влияние информационной войны на психологическое состояние человека и его поведение в обществе. Анализируются методы и техники, используемые в информационных войнах. Обсуждаются психологические механизмы, которые делают людей уязвимыми перед информационными атаками, а также их последствия для социального взаимодействия. Предлагаются рекомендации по снижению негативного воздействия информационных войн на человека.
Ключевые слова: *информационная война, психологическое состояние, поведение в обществе, информационные атаки, уязвимость, социальное взаимодействие, воздействие на человека.*

В эпоху цифровых технологий и мгновенного обмена информацией, понятие когнитивной войны становится все более актуальным. Однако за кулисами хакерских атак и массового распространения заведомо ложных новостей, скрывается нечто более глубокое – воздействие на психику человека и его поведение в обществе. По словам Наталии Красовской, политического психолога, кандидата психологических наук, информационная война – «борьба за умы людей, наносящая обществу тяжёлую культурно-психологическую травму, от которой очень сложно оправиться» [3]. Информация проникает в повседневную жизнь людей, сказываясь на их психологическом состоянии и поведенческих реакциях. Она способствует усилению поляризации общества, разделяя людей на группы с противоположными взглядами и усиливая конфликты. Чрезмерное воздействие манипулятивных техник приводит к изменению восприятия реальности и формированию мнений, подкрепленных ложными фактами. Постоянный поток негативной информации может снизить мотивацию людей к участию в общественной жизни из-за ощущения бесполезности и безысходности. Множество источников, часто представляющих противоречивые сообщения, создают путаницу, вносят неопределенность и стресс в сознание индивида. Этот феномен, оказывая давление на человека и его поведение в обществе, становится предметом все более широкого изучения и вызывает растущий интерес среди исследователей, практиков и общественности в целом.

Когнитивная война представляет собой стратегический подход, в рамках которого информационные ресурсы используются для воздействия на мышление человека, изменение его ценностей и поляризацию необходимо-

го мнения в обществе с целью достижения определенных политических, экономических или военных целей. В отличие от традиционных форм конфликтов, информационная война оперирует не столько физической силой, сколько влиянием на противника, манипуляцией фактами и формированием определенных представлений. Основные способы включают в себя использование различных медиа-платформ, социальных сетей, новостных и интернет-источников для распространения специально подобранной информации, которая может быть как правдивой, так и ложной, но ее основная задача – воздействовать на восприятие и убеждения аудитории. Этот вид конфликта, обладающий множеством тонких методов и стратегий, часто бывает невидимым и не ограничивается территориальными границами, что делает его особенно сложным для обнаружения и противодействия.

Опасность информационной войны не ограничивается лишь поверхностным воздействием, ее последствия проникают глубже. Массовые манипуляции, вызванные фальсификациями и приводящие к формированию определенных стереотипов или предубеждений, могут создать атмосферу неопределенности, страха и подрыва доверия к новостным источникам. Кроме того, кибератаки, характерные для данных войн, представляют серьезную угрозу для стабильности и безопасности, ведь возможность осуществления атак на системы государства и предприятий могут привести к дестабилизации экономики и общества в целом. Таким образом, война выходит за пределы простого воздействия на информационные потоки, что требует разработки эффективных методов противостояния.

В наше время, когда информация представляет собой огромный поток данных, все сложнее отфильтровать её для обработки. Выделить необходимую информацию становится труднее из-за насыщенности лозунгами, агитацией и пропагандой. Очевидно, что влиять на людей легко, если знать, как это делать правильно. Наше сознание постоянно подвергается попыткам манипуляции через различные методы и техники. Чтобы противостоять им, необходимо уметь распознавать различные виды и способы пропаганды. Один из ключевых подходов заключается в использовании авторитетных личностей или групп влияния для привлечения внимания целевой аудитории. Эти авторитеты могут включать в себя известных политических деятелей, руководителей предприятий, преподавателей высших и средних учебных заведений, деятелей культуры, известных актеров. Эффективность этого метода зависит от уровня доверия, который представитель группы влияния имеет у целевой аудитории, а также от степени его известности. Так, в ходе избирательных кампаний часто привлекают известных артистов, которые активно поддерживают того или иного кандидата. В ряде случаев они даже вступают в состав определенных политических движений, что способствует улучшению репутации этих движений. Например, в 1992 году известный киноактер Арнольд Шварцнеггер выступил в поддержку Джорджа Буша на выборах Президента США.

Помимо основного подхода, существуют и другие теории информационных войн, представляющие разнообразные стратегии и тактики. Одной

из таких теорий является «Имитационная дезинформация». Этот подход включает в себя изменение пропаганды противоположной стороны с целью снижения доверия к ней и формирования негативного образа. Другой теорией является «Псевдологические выводы», которая основана на использовании ложных выводов, которые преподносятся как логически верные, для воздействия на мнение целевой аудитории. Также существует «Принуждающая пропаганда», воздействующая на общественное мнение через использование слов и выражений с принуждающим характером. К таковым можно отнести расклеивание листовок или распространение сообщений с агитацией к какому-либо действию. Наибольшую популярность в наши дни набирает способ воздействия на общество с помощью «Массовых вбросов». Они характеризуются резким заполнением всевозможных источников информацией, которая носит яркий эмоциональный окрас и нередко является профессионально переработанной правдой в негативном ключе. Таким образом, видя подобную новость и слепо доверяя ей, основываясь на том, что о ней говорят массово, люди становятся более уязвимыми и легче поддаются на дальнейшие уловки, поэтому при восприятии известий, которые внезапно появляются на множестве ресурсов и вызывают широкий спектр эмоциональных реакций от сочувствия до негодования, важно осознавать возможность попадания под воздействие информационного вброса. Присутствие хорошо структурированной текстовой составляющей и эмоциональная насыщенность часто являются признаками данного явления.

В связи с последними событиями, касающимся всего мира в целом, психологи считают: «Субъективно можно сказать, судя по поведению людей в социальных сетях, цифровых платформах и мессенджерах, – многие в моральной панике». Социальные сети полны «свидетельств с мест», когда показывают настоящие и ненастоящие фото и видео с подачей нужной интерпретации, что является инструментом информационной войны и ведет к появлению хаоса и морального дисбаланса.

Чтобы сделать общество более устойчивым к информационным атакам, необходимо принимать комплекс мер, охватывающих различные аспекты образования, информационной грамотности, технических защит и сознательной критической мысли. Важным шагом является повышение информационной грамотности, которое включает в себя не только умение различать достоверные и ложные источники информации, но и анализ контента, осознание мотивов за информационными кампаниями и развитие способности к самокритике. Образовательные программы, медиаобразование и обучение критическому мышлению играют ключевую роль в формировании у общества этих навыков. Но тем не менее не стоит забывать о важности современных средств киберзащиты от хакерских атак, укреплении сетевой безопасности и разработки механизмов фильтрации информации для идентификации и блокировки нежелательных искаженных сообщений. Помимо этого, важно поощрять активное участие граждан в общественной жизни и укреплять доверие к независимым источникам инфор-

мации. Создание и поддержка платформ для обсуждения и диалога, где каждый может высказать свою точку зрения, а также поощрение медиа, следующих высоким журналистским стандартам, способствуют формированию здоровой информационной среды.

Однако, абсолютной защиты от информационной войны не существует. «Вы не избежите информационного влияния, так как мы постоянно потребляем новости и различный политический контент», – говорит социальный психолог, Михаил Вершинин [2]. Вместо этого необходимо стремиться к созданию устойчивого общества, осознающего свои слабые места и способное реагировать на вызовы информационных атак. Реализация этих мер поможет создать более устойчивое и информированное общество, способное противостоять информационным угрозам в современном мире.

Список литературы

1. Сулейманова Ш.С., Назарова Е.А., Информационные войны: история и современность: Учебное пособие. – М.: Международный издательский центр «Этносоциум», 2017. 124 с. URL: https://mgimo.ru/upload/iblock/486/%D0%A1%D1%83%D0%BB%D0%92%D0%9D%D0%AB.pdf.

2. Социальный психолог Михаил Вершинин о том, как не стать жертвой информационной войны – Рамблер/финансы (rambler.ru) URL: https://finance.rambler.ru/money/48236315-sotsialnyy-psiholog-mihail-vershinin-o-tom-kak-ne-stat-zhertvoy-informatsionnoy-voyny/?ysclid=lp5xsfa15z362935336.

3. «Им нужен ваш мозг»: как влияют на человечество информационные войны | ПОЛИТИКА | АиФ Новосибирск (aif.ru) URL: https://nsk.aif.ru/politic/im_nuzhen_vash_mozg_kak_vliyayut_na_chelovechestvo_informacionnye_voyny?ysclid=lp5xpshpno772970789.

4. Федорова О. Н. Информационно-психологическая безопасность личности в информационном обществе / О. Н. Федорова // Вестник Дальневосточного государственного технического университета. – 2011. – № 2(7). – С. 21-34. – EDN SZGXNT. URL: https://www.elibrary.ru/download/elibrary_22541053_37046639.pdf.

5. Джура Г. С. Информационно-психологическая безопасность личности в современных реалиях / Г. С. Джура // Вестник Донецкого национального университета. Серия Д: Филология и психология. – 2022. – № 3. – С. 119-122. – EDN TZUVUY. URL: https://www.elibrary.ru/download/elibrary_53876141_58059365.pdf.

6. Ряжапов Н. Х. Национальные интересы России в информационной сфере в условиях мировой нестабильности и меры их обеспечения / Н.Х. Ряжапов // Развитие науки и образования в условиях мировой нестабильности: современные парадигмы, проблемы, пути решения: Материалы Международной научно-практической конференции. В 2-х частях, Ростов-на-Дону, 29 октября 2021 года. Том Часть 1. – Ростов-на-Дону: ООО «Из-

дательство ВВМ», 2021. – С. 101-110. – EDN ESSRPG. URL: https://www.elibrary.ru/download/elibrary_47231698_67351052.pdf.

7. Морозов А. В. Психология информационной провокации / А. В. Морозов // Казанский педагогический журнал. – 2017. – № 6(125). – С. 27-35. – EDN ZTWRGP. URL: https://www.elibrary.ru/download/elibrary_30611528_51412637.pdf.

8. Манойло А. В. Информационные войны / А. В. Манойло // Геополитический журнал. – 2017. – № 5-6(20). – С. 28-36. – EDN YVAZFA. URL: https://www.elibrary.ru/download/elibrary_32751839_91412484.pdf.

INFORMATION AND PSYCHOLOGICAL IMPACT ON A PERSON IN MODERN SOCIETY

D.S. Malikov, A.A. Nekrasov
Perm Military Institute of the National Guard Troops of Russian Federation

Abstract. This paper examines the impact of information warfare on the psychological state of a person and his behavior in society. The methods and techniques used in information wars are analyzed. The psychological mechanisms that make people vulnerable to information attacks, as well as their consequences for social interaction, are discussed. Recommendations are offered to reduce the negative impact of information wars on humans.

Keywords: *Information war, psychological state, behavior in society, information attacks, vulnerability, social interaction, human impact.*

ИСПЫТАНИЕ АНТИВИРУСНОГО СРЕДСТВА ПО ОБНАРУЖЕНИЮ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ФОРМАТА PORTABLE EXECUTABLE

И.Н. Захарова, С.С. Матовых, А.А. Отамбаев, И.А. Терновой
Академия Федеральной службы охраны России

Аннотация. В данной статье проведена оценка эффективности использования антивирусного решения Kaspersky Endpoint Security для обнаружения вредоносного программного обеспечения (ПО) формата Portable Executable (PE). Проведенные эксперименты показали, что антивирусные средства без использования онлайн-сервисов и актуальных обновлений демонстрируют низкую эффективность. Результаты подчеркивают важность регулярного обновления баз данных и использования облачных технологий для повышения эффективности обнаружения вредоносного ПО.
Ключевые слова: *кибербезопасность, вредоносное ПО, Portable Executable, антивирусные базы данных, облачные технологии.*

Введение

В современном цифровом мире стремительный рост кибератак и увеличение числа новых вариантов вредоносного программного обеспечения создают серьезные вызовы для безопасности информационных систем. Современные вредоносные программы активно используют методы обфускации, упаковки и полиморфизма, которые затрудняют их обнаружение традиционными методами. Это требует использования более совершенных подходов к обнаружению вредоносного ПО, включающих поведенческий анализ, машинное обучение и облачные технологии [1].

Цель настоящего исследования – оценка эффективности антивирусного средства Kaspersky Endpoint Security для обнаружения вредоносного ПО формата PE [2], с учетом влияния актуальности обновления баз данных и использования облачных технологий. Проведенное исследование направлено на выявление зависимости между этими факторами и точностью обнаружения вредоносного ПО, что особенно актуально для применения в корпоративных и государственных информационных системах, где требуется высокий уровень информационной безопасности.

Ранее проведённые исследования [3-4] подтвердили важность регулярного обновления баз данных и использования облачных технологий для повышения эффективности защиты от вредоносного ПО. В частности, работа Тетериной Е.В. и Черненко В.В. [3] показала, что антивирусные продукты, такие как Kaspersky Internet Security и Dr.Web, демонстрируют высокие показатели самозащиты при условии регулярных обновлений и использова-

ния современных механизмов защиты. Исследование Калашниковой А.А. и соавторов [4] предложило методику сравнительного тестирования антивирусных решений, основанную на таких критериях, как уровень детектирования вирусов, процент ложных срабатываний и эффективность эвристического анализа, что позволяет объективно оценивать современные антивирусные продукты в условиях постоянно меняющихся киберугроз. Методика, разработанная Беловым А.С., Добрышиным М.М. и Шугуровым Д.Е. позволяет на основе учета динамики объема используемых вычислительных ресурсов и изменения количества определенных видов компьютерных атак прогнозировать изменение эксплуатационных характеристик [5].

Испытательный стенд и методика проведения испытаний

Для исследования выбрано антивирусное решение Kaspersky Endpoint Security по нескольким причинам. Соответствие требованиям государственных органов РФ. Kaspersky Endpoint Security имеет сертификаты соответствия Федеральной службы по техническому и экспортному контролю (ФСТЭК России) и Федеральной службы безопасности (ФСБ России), что позволяет использовать его в информационных системах государственных органов [6]. Технологическое преимущество в использовании передовых технологий, включая облачную инфраструктуру Kaspersky Security Network (KSN), проактивные методы обнаружения и поведенческий анализ, обеспечивает высокую эффективность в детектировании современных киберугроз.

В данном исследовании использовался набор вредосного ПО скачанный с сайта Virusshare [7] архив вирусов VirusShare_00486.rar (20,29 Гб) от 14.02.2024 г. содержащий 65536 вредоносных файлов различных типов (вирусы, трояны, черви, эксплойты и др.). Из этого архива было выделено 18211 файлов формата Portable Executable (PE) (формат PE32 – 16496, формат PE64 – 1715), которые стали объектом анализа. Формат PE широко используется в операционных системах Windows и содержит необходимую информацию для загрузки и исполнения кода, что делает его критически важным для анализа безопасности.

Методология проведения экспериментов

Эксперименты проводились с целью определения эффективности антивирусного средства при различных конфигурациях, включая версию базы данных и использование облачных технологий. Каждый эксперимент проводился в три этапа:

1. На первом этапе создавалась контролируемая виртуальная тестовая среда на базе VMware Workstation версии 16.1.2. Что позволило смоделировать работу антивирусного решения без риска для реальной системы. Для каждого эксперимента клонировалась «чистая» виртуальная машина, что обеспечивало последовательность и исключало влияние предыдущих тестов.

В качестве операционной системы использовалась Windows 10 Pro с последними обновлениями, что обеспечило реалистичную платформу для

тестирования. Антивирусное решение Kaspersky Endpoint Security было развернуто с различными версиями баз данных, а тесты проводились как с активацией KSN, так и без нее.

Для обеспечения целостности данных контрольные суммы файлов проверялись с помощью программы Hash Check, подтверждая, что файлы оставались неизменными на протяжении всего процесса тестирования.

2. На втором этапе на подготовленную виртуальную машину загружались вредоносные файлы, после чего в ручном режиме запускалось антивирусное сканирование директории. В ходе сканирования фиксировались обнаруженные угрозы, определялся их тип и проверялись контрольные суммы SHA-256 для подтверждения целостности файлов. В экспериментах использовались различные версии баз данных с целью оценки влияния их актуальности на результаты сканирования.

3. На третьем этапе производился сбор и обработка данных. Анализировалась эффективность обнаружения в зависимости от типа угрозы и от конфигурации системы (использование облачных технологий KSN или работа в автономном режиме). Для количественной оценки использовались метрики: версия используемой базы данных, использование облачных технологий KSN и процент обнаруженных угроз.

Важным элементом экспериментов было использование облачной инфраструктуры KSN. В половине экспериментов антивирусное средство работало без подключения к KSN, полагаясь исключительно на локальные базы данных, что позволило оценить его возможности в автономном режиме. В остальных экспериментах KSN использовался для получения обновленных данных о вредоносных программах, что значительно повышало эффективность обнаружения новых и изменённых угроз.

Результаты исследования

Результаты проведенных экспериментов представлены в Таблице и продемонстрировали существенную разницу в точности обнаружения вредоносных программ при использовании антивирусных баз данных и облачных технологий. Использование базы данных за февраль 2021 года без использования облачных технологий KSN привело к обнаружению лишь 54,4% вредоносных файлов. Это подтверждает необходимость регулярного обновления баз данных для эффективного обнаружения новых угроз. В экспериментах 2, 3, 5, 7 с обновленными базами данных, существенно увеличилась точность обнаружения, однако без использования облачных технологий KSN остаётся значительное количество не обнаруженных угроз. В экспериментах 4, 6, 8 использование облачных технологий KSN вместе с обновленными базами данных повысило эффективность обнаружения до более 90%. Это показывает, что облачные технологии значительно улучшают обнаружение современных угроз.

Таблица

Результаты эксперимента по определению эффективности антивирусного средства

№ п/п	Версия баз данных	Использование KSN	Обнаружено вредоносных файлов (%)
1	25.02.2021	Нет	54,4%
2	19.02.2024	Нет	73,6%
3	03.04.2024	Нет	75,6%
4	03.04.2024	Да	90,7%
5	05.05.2024	Нет	75,7%
6	05.05.2024	Да	90,8%
7	05.10.2024	Нет	85,3%
8	05.10.2024	Да	95,5%

Заключение

Проведённое исследование подтвердило, что эффективность Kaspersky Endpoint Security в обнаружении вредоносного ПО формата PE существенно зависит от актуальности баз данных и использования облачных сервисов KSN. Без регулярных обновлений и интеграции облачных технологий эффективность обнаружения снижается, что увеличивает риски для информационной безопасности. В дальнейшем предполагается продолжить исследования в области машинного обучения для повышения адаптивности антивирусных систем к новым угрозам и улучшения показателей обнаружения вредоносного ПО.

Список литературы

1. Лаборатория Касперского. Технологии обеспечения безопасности. [Электронный ресурс] / URL: https://www.kaspersky.ru/enterprise-security/wiki-section/home (дата обращения: 25.11.2024)

2. Майкрософт. «Описание формата Portable Executable.» Microsoft Developer Network. [Электронный ресурс] / URL: https://docs.microsoft.com/ru-ru/windows/ win32/debug/pe-format (дата обращения: 18.08.2024).

3. Тетерина, Е. В. Анализ эффективности работы современных антивирусных программ / Е. В. Тетерина, В. В. Черненко // Решетневские чтения. – 2010. – Т. 2. – С. 559-560. EDN: UNKLOL

4. Разработка методики сравнительного тестирования антивирусных продуктов / А. А. Калашникова, Д. А. Калинин, А. В. Клейменов [и др.] // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. – 2008. – № 52. – С. 283-289.

5. Методика прогнозирования и оценки эксплуатационных характеристик программных средств защиты от компьютерных атак в течение заданного времени эксплуатации / Белов А.С., Добрушин М.М., Шугуров Д.Е. // Известия Тульского государственного университета. Технические науки. – 2024. – № 2. – С. 225-229. DOI: 10.24412/2071-6168-2024-2-225-226 EDN: TZEAKE

6. ФСТЭК России. Реестр сертифицированных средств защиты информации. [Электронный ресурс] / URL: https://reestr.fstec.ru/reg3 (дата обращения: 26.11.2024)

7. VirusShare.com. A collection of malware samples for research purposes. [Электронный ресурс] / URL: https://virusshare.com/torrents (дата обращения: 14.02.2024).

TESTING OF AN ANTIVIRUS TOOL FOR DETECTING MALICIOUS SOFTWARE IN THE PORTABLE EXECUTABLE FORMAT

I.N. Zakharova, S.S. Matovikh, A.A. Atambayev, I.A. Ternovoy
Russian Federation Security Guard Service Federal Academy

Abstract. This article evaluates the effectiveness of using Kaspersky Endpoint Security antivirus solution to detect malware in Portable Executable (PE) format. Experiments have shown that antivirus tools without using online services and current updates demonstrate low efficiency. The results highlight the importance of regularly updating databases and using cloud technologies to improve malware detection efficiency.

Keywords: *cybersecurity, malware, Portable Executable, antivirus databases, cloud technologies.*

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МОДЕЛЕЙ КОМПЬЮТЕРНЫХ ВИРУСОВ

И.Н. Захарова, С.С. Матовых, А.В. Метыкова, А.О. Отамбаев
Академия Федеральной службы охраны России

Аннотация. В данной статье представлен сравнительный анализ моделей компьютерных вирусов, используемых для изучения и предотвращения их распространения в цифровых системах. Рассматриваются различные подходы к моделированию, особое внимание уделяется характеристикам и условиям применения. Оцениваются достоинства и недостатки каждой модели.

Ключевые слова: *компьютерный вирус, программа, информационная безопасность, модель.*

Введение

В современном цифровом мире компьютерные вирусы представляют собой одну из самых серьезных угроз для информационной безопасности. С развитием технологий и увеличением числа подключенных к сети устройств, атаки злоумышленников становятся все более разнообразными. Для эффективной защиты компьютерных систем необходимо не только своевременно выявлять и устранять уязвимости, но и предугадывать возможные пути распространения вредоносного ПО [1]. В связи с этим актуальным становится использование различных моделей для анализа и предсказания поведения компьютерных вирусов. Существует множество подходов к моделированию вирусных атак.

Рассмотрим некоторые модели вирусов, их условия применения, достоинства и недостатки.

Модель Ф. Коэна

Первая формально определенная модель вируса была предложена в докторской диссертации Ф. Коэна и получила известность благодаря использованию ее в статьях «Компьютерные вирусы: теория и эксперименты» [2] и «Вычислительные аспекты компьютерных вирусов» [3] в 1984 году. Определение вируса- «паразита» по Ф. Коэну: компьютерный вирус – программа, которая может заражать другие программы, модифицируя их таким образом, чтобы внедрять в них собственную, возможно видоизмененную, копию.

Модель Ф. Коэна была создана для формального описания и изучения распространения компьютерных вирусов. Она не является моделью конкретного вируса, а представляет собой абстрактную математическую модель, позволяющую понять, как вирус может заражать другие программы и системы. Основная цель – доказать возможность создания самовос-

производящихся программ, способных распространяться по компьютерной системе без явного участия пользователя.

Для эффективного применения модели Ф. Коэна необходимо учитывать некоторые условия:

– Определение среды распространения: модель предполагает наличие вычислительной среды, в которой вирусы могут распространяться. Это может быть компьютерная сеть или отдельные системы, которые допускают выполнение программного кода.

– Автономное выполнение кода: для реализации модели важно, чтобы вирус мог автономно исполнять свой код на зараженной системе. Это означает, что вирусу необходимо иметь возможность копировать себя и запускаться без вмешательства пользователя.

– Наличие средств защиты: для оценки эффективности модели должны учитываться существующие средства защиты и противодействия.

Данная модель вирусов базировалась на способе описания алгоритмов при помощи «машины Тьюринга». «Машина Тьюринга» определяется:

– S = {s1, s2, … sn} – множеством состояний, в которых она может находиться;

– I = {i1, i2, … im} – алфавитом данных, записанных на ленте;

– N: S × I → S, O: S × I → I, D: S × I → d – набором инструкций, которые в зависимости от текущего состояния «машины» и данных в текущей ячейке ленты устанавливают новое состояние, изменяют данные на ленте и определяют перемещение d = {–1, 0, +1} головки чтения-записи относительно ее текущего положения.

Ф. Коэн рассматривал не все возможные «машины Тьюринга», а только те из них, данные на ленте которых предназначены для дальнейшей «интерпретации», то есть сами представляют собой программы. Он ввел три дополнительные функции: 8(N): N → S – состояние машины после N-го шага работы; Q (N): N × N → I – содержимое указанной ячейки после указанного шага и P(N): N → N – значение следующего номера ячейки после выполнения указанного шага. В совокупности эти функции представляют собой «историю поведения» машины, и с их помощью Коэн составил определение «вирусного множества» VS, то есть множества V компьютерных вирусов для «машины Тьюринга» M.

Таким образом, Ф. Коэн определил «вирусное множество» как множество «машин Тьюринга», способных перемещать записи на своей ленте из одного места в другое.

Достоинства модели Ф. Коэна:

– возможность исследования с ее помощью некоторых важных свойств, которыми обладают как «математические», так и «настоящие» вирусы;

– возможность написания последовательности инструкций, которая строит на ленте данных копии для любой конечной последовательности символов;

– вывод о том, что не существует алгоритма, способного обнаруживать множество всех возможных компьютерных вирусов (это позволяет без особых разбирательств отметать любые заявления о создании алгоритма, точно детектирующего вирусы).

Недостатки модели Ф. Коэна:

– невозможность надёжного распознавания вирусов;

– невозможность анализа кода без его запуска.

Таким образом, модель Ф. Коэна стала важным шагом в развитии области кибербезопасности, предоставив исследователям и специалистам по информационной безопасности инструменты для анализа и борьбы с компьютерными угрозами.

Модель Л. Адлемана

Известный специалист в области защиты информации Л. Адлеман в своей статье «Абстрактная теория компьютерных вирусов» (1988г.) определил компьютерный вирус-«паразит» через понятие «заражения» [4]. В основе модели Л. Адлемана лежит тезис о том, что для каждой программы возможны как «здоровая», так и «зараженная» формы, и, соответственно, существует некая функция, преобразующая программу из первой формы во вторую. Эту функцию (а точнее алгоритм, ее вычисляющий) Л. Адлеман и ассоциировал с «компьютерным вирусом». Однако самое главное, ради чего Л. Адлеман разрабатывал свое определение, – это изучение возможности различения «зараженных» и «здоровых» программ.

Условия применения модели вирусов Л. Адлемана:

– Самовоспроизводство: модель должна описывать способ, которым вирус может копировать себя и распространяться на другие программы или файлы.

– Скрытность: модель должна объяснять, как вирус может скрывать свое присутствие от пользователей и антивирусных программ.

– Условие запуска: описание того, какие условия должны быть выполнены для активации вируса или его распространения. Это может быть дата, действие пользователя или наличие определенного программного обеспечения.

– Межсетевое взаимодействие: в современном мире модель должна также учитывать, как вирусы распространяются через сетевые соединения и как они могут взаимодействовать или координировать свои действия через Интернет.

За математическую основу Л. Адлеман взял «Геделевские нумерации» – остроумный способ пронумеровать каждый знак (включая цифры, буквы, знаки арифметических действий, кванторы и т. п.) и, произведя над ними определенные действия, получить для каждого математического выражения его уникальный номер – так называемый «Геделев номер», или «нумерал». Далее Л. Адлеман определил отношение «подобия с точностью до функции h». По Л. Адлеману, два числа p и q «подобны с точностью до h», если два алгоритма, нумералами которых эти числа являются, либо в

точности совпадают, либо содержат элементы-суперпозиции с h. И использовав принятую в теории алгоритмов нотацию обозначения рекурсивных функций φ_p = φ(p), Адлеман составил следующее определение. Для всех Геделевских нумераций частично рекурсивных функций {ϕi} полностью определенная рекурсивная функция v является вирусом по отношению к {ϕi} только тогда, когда для всех d, p ϵ S:

1) либо ∀i, j ϵ N: ϕv(i)(d, p) = ϕv(j)(d, p) – то есть после заражения выполняется совсем иной, не предусмотренный в программе алгоритм;

2) либо ∀j ϵ N: ϕj(d, p) ≅ ϕv(j)(d, p) – то есть алгоритмы работы исходной и зараженной программ «подобны с точностью до вирусного преобразования v», где S – множество всевозможных конечных последовательностей натуральных чисел, p – программный код, d – не подверженные инфицированию «данные».

Достоинства модели Л. Адлемана:

– простота и понятность;
– математическая строгость;
– предсказательная способность.

Недостатки модели Л. Адлемана:

– ограниченная точность;
– недостаточная детализация;
– невозможность описания сложных взаимодействий.

Таким образом, модель компьютерных вирусов Л. Адлемана является простой и понятной моделью, которая может быть полезна для начала изучения компьютерных вирусов. Однако, из-за ограниченной точности, недостаточной детализации и невозможности описания сложных взаимодействий, она не может быть использована как единственная модель для описания поведения вирусов в реальных системах.

«Французская» модель

Модель, французских авторов Ж. Бонфана, М. Качмарека и Ж-И. Мариона, была рассмотрена в статьях «Абстрактное детектирование компьютерных вирусов» [5] и «Классификация вирусов при помощи теоремы о рекурсии» [6] в 1989 году. Данная модель представляет собой одну из первых попыток формализовать поведение компьютерных вирусов и их распространение в сетях.

Условия применения «французской» модели вирусов:

– Наличие уязвимостей: модель предполагает, что в системе существуют уязвимости, которые вирус может использовать для заражения. Это могут быть ошибки в программном обеспечении, неправильные настройки безопасности или действия пользователя.

– Возможность заражения: вирус должен иметь возможность заражать другие программы или файлы. Это может происходить путем внедрения вредоносного кода в исполняемые файлы, документы или другие типы данных.

– Возможность размножения: вирус должен иметь возможность размножаться внутри системы. Это может происходить путем создания копий самого себя или заражения других файлов.

В математической основе данной модели лежит известная в теории алгоритмов «теорема Клини»: для любой частично рекурсивной функции g одного аргумента всегда найдется такое натуральное n («неподвижная точка»), что n = g(n). Зная, что n может играть роль «нумерала» какой-нибудь иной функции или алгоритма, можно обобщить эту формулировку до вида: $\varphi_e(x) = g(e, x)$, где x – произвольный аргумент функции или набор данных для программы, e – некий алгоритм, а $\varphi_e = \varphi(e)$ – программа, полученная в результате записи ее алгоритма на языке j.

Достоинства «французской» модели:

– возможность более точной оценки сложности распознающих алгоритмов;

– модель позволяет теоретически обосновать корректность реально применяемых методов антивирусной борьбы;

– модель предоставляет четкие определения и математические формулировки, что позволяет точно описывать процессы заражения и распространения вирусов;

– возможность применения к различным типам вирусов и сетевых структур, что делает её универсальной.

Недостатки «французской» модели:

– более теоретическая модель и может не предоставлять конкретные практические инструменты для борьбы с вирусами;

– применение модели на практике может требовать значительных вычислительных ресурсов и специализированных знаний.

Таким образом, «французская» модель компьютерных вирусов является важным вкладом в теорию кибербезопасности. Она предоставляет ценные инструменты для анализа и понимания распространения вирусов, но имеет ограничения в плане практической применимости и учета современных сложных угроз.

Модель китайских авторов Z. Zuo и M. Zhou

Модель компьютерных вирусов, разработанная китайскими исследователями Z. Zuo и M. Zhou, является важной работой в области моделирования, распространения вредоносного программного обеспечения. Модель основана на классической эпидемиологической модели SIR (Susceptible-Infected-Recovered), адаптированной для компьютерных сетей.

Условия применения:

– компьютерные сети с достаточно большим количеством узлов;

– ситуации, где можно четко разделить компьютеры на категории: уязвимые, зараженные и восстановленные;

– сценарии, где скорость распространения вируса и эффективность антивирусных мер могут быть количественно оценены.

Эта модель использует правила, принятые в теории рекурсивных функций, и является расширением модели Л. Адлемана. В модели китайских авторов Z. Zuo и M. Zhou программы рассматриваются как векторы из множества элементов: $p = (i_1, i_2, \ldots, i_n)$, причем для обозначения программ с видоизмененными элементами используется нотация $p[j_k/i_k] = (i_1, i_2, \ldots, j_k, \ldots, i_n)$, а для указания функции, которая произвела эту модификацию, используется обозначение $p[v(i_k)] = p[v(i_k)/i_k] = (i_1, i_2, \ldots, v(i_k), \ldots, i_n)$. Такой подход позволил авторам конкретизировать, какой именно элемент модифицируется вирусом в программе или операционной системе в результате заражения, и выделить различные типы вирусов.

Достоинства:

– адаптация классической эпидемиологической модели к компьютерным сетям;

– учет специфических факторов распространения компьютерных вирусов;

– возможность прогнозирования динамики распространения вирусов;

– относительная простота модели, позволяющая применять ее в различных сценариях.

Недостатки:

– не учитываются все возможные варианты поведения современных вирусов и вредоносных программ;

– может не отражаться специфика некоторых типов сетей или особых видов вирусов;

– может потребоваться значительная адаптация для применения к конкретным ситуациям;

– не учитываются сложные взаимодействия между различными типами вредоносного ПО.

Таким образом, модель Zuo и Zhou предоставляет полезный инструмент для понимания и анализа распространения компьютерных вирусов, но её применение требует понимания её ограничений и возможной необходимости дополнения другими методами анализа для получения более полной картины.

Векторная модель Д. Зегжды

Векторная модель компьютерных вирусов, разработанная российским ученым Д.П. Зегждой [7]. Модель была представлена в ряде научных работ и учебных пособий автора, в том числе в книге «Основы безопасности информационных систем» (соавторы Д.П. Зегжда, А.М. Ивашко), изданной в 2000 году.

Данная модель предоставляет мощный инструмент для анализа и прогнозирования поведения компьютерных вирусов. Она позволяет более точно оценивать риски и разрабатывать эффективные меры защиты, что особенно важно в условиях постоянно эволюционирующих киберугроз.

Условия применения векторной модели Д. Зегжды:

– Анализ угроз: модель может использоваться для анализа потенциальных угроз и определения наиболее уязвимых узлов в сети.

– Образовательные цели: модель помогает в обучении специалистов по кибербезопасности пониманию сложных взаимосвязей в распространении вирусов.

– Разработка защитных мер: используется для разработки эффективных стратегий защиты, основанных на анализе векторов уязвимостей.

В данной модели как «нормальная» программа, так и вирус представлены в виде векторов. Процесс заражения вирусом V программы P происходит в результате последовательного выполнения трех функций: P'= I(D(P), A(V)), где D – «возмущение», то есть подготовка программы к заражению, например коррекция в заголовке EXE-программы адреса точки входа или переписывание начала COM-программы в ее конец; A – создание копии вируса, подготовленной для внедрения в конкретную программу, например содержащей в «загашнике» старое значение адреса точки входа из заголовка EXE-программ; I – инфицирование, вписывание вирусной копии внутрь программы. Также автор предположил, что «тело» вируса есть A(V) = Q(V) + S(V), где Q – настраиваемая часть вируса, S – постоянная часть вируса, «+» – обобщенная операция «встраивания» одного вектора в другой.

Достоинства векторной модели Д. Зегжды:

– Гибкость: модель позволяет учитывать множество факторов и параметров.

– Детальность: обеспечивается подробное описание поведения вирусов.

– Прогнозирование: возможность предсказания развития вирусных атак.

– Адаптивность: модель может быть настроена для различных типов вирусов и систем.

Недостатки векторной модели Д. Зегжды:

– Сложность: могут потребоваться значительные вычислительные ресурсы.

– Необходимость точных данных: эффективность зависит от качества входных параметров.

– Абстрактность: некоторые аспекты реального поведения вирусов могут быть упрощены.

Таким образом, модель Д. Зегжды представляет собой важный шаг в развитии теоретических основ информационной безопасности, объединяя математический подход с практическими аспектами компьютерной вирусологии.

Заключение

В данной статье был проведен сравнительный анализ различных моделей компьютерных вирусов. Исследование охватило модели Ф. Коэна, Л. Адлеиана, Z. Zuo и M. Zhou, Д. Зегжды и «французскую», сравнение ко-

торых осуществлялось по нескольким критериям. Результаты анализа показали, что каждая из рассмотренных моделей обладает своими преимуществами и недостатками, а выбор оптимальной зависит от конкретных задач исследования и типа анализируемого вируса. Дальнейшие исследования в этой области могут быть направлены на создание гибридных моделей, интеграцию с методами искусственного интеллекта и разработку новых подходов к моделированию современных угроз информационной безопасности.

Список литературы

1. Компьютерные вирусы и антивирусы: взгляд программиста: учебное пособие / К.Е. Климентьев. – М.: ДМК Пресс, 2013. – 656 с. ISBN: 978-5-94074-885-4 EDN: ZGXCPX

2. Cohen F. Computer viruses: theory and experiments / Computers and Security, Vol. 6, 1987. – P. 22–35. DOI: 10.1016/0167-4048(87)90122-2

3. Cohen F. Computational aspects of computer viruses / Computers and Security, Vol. 8, 1089. – P. 325–344.

4. Adleman L. An Abstract Theory of Computer Viruses / CRYP – TO ‘88. – P. 354–374.

5. Bonfante G., Kaczmarek M., Marion J.-Y. Abstract detection of computer viruses / Munich, APPSEM II, 2005.

6. Bonfante G., Kaczmarek M., Marion J.-Y. A Classification of viruses through recursion theorems / CiE, 2007 – P. 73–82. DOI: 10.1007/978-3-540-73001-9_8 EDN: YCGFVJ

7. Зегжда Д. Векторно-операторная модель компьютерных вирусов / Компьютер Пресс. – 1993. – № 10. – С. 47–48.

COMPARATIVE ANALYSIS OF MODELS COMPUTER VIRUSES

I.N. Zakharova, S.S. Matovikh, A.V. Matykova, A.A. Atambayev
Russian Federation Security Guard Service Federal Academy

Abstract. This article presents a comparative analysis of computer virus models used to study and prevent their spread in digital systems. Various approaches to modeling are considered, special attention is paid to the characteristics and conditions of application. The advantages and disadvantages of each model are evaluated.

Keywords: *computer virus, program, information security, model.*

ВЫЯВЛЕНИЕ ДИСКРЕДИТИРУЮЩЕЙ ИНФОРМАЦИИ В КИБЕРПРОСТРАНСТВЕ: СОВРЕМЕННЫЕ ВОЗМОЖНОСТИ

В.А. Минаев, А.С. Коломина
Московский университет МВД им. В.Я. Кикотя

Аннотация. Рассмотрены вопросы выявления, анализа и предотвращения угроз дискредитации организаций и конкретных индивидов с использование социальных медиа. Обращается внимание на применение математических методов и моделей при описании процессов распространения дискредитирующей информации. Дается определение, обсуждаются основные формы и приводятся примеры дискредитации. Показана роль социальных медиа в системе реализации дискредитирующих воздействий. Делается вывод о том, что в условиях роста информационных вызовов и усложнения цифровых рассмотренные методы и модели становятся незаменимыми инструментами для защиты репутации, обеспечения доверия к медиа информации.
Ключевые слова: *угрозы дискредитации, социальные медиа, дискредитирующая информация, дискредитирующие воздействия.*

Введение

Киберпространство, являясь ключевым элементом современной информационной среды, продолжает стремительно развиваться. С его расширением открываются не только новые возможности для коммуникации, сотрудничества и обмена данными, но и возрастают угрозы, связанные с деструктивным использованием цифровых технологий [1]. Одной из значимых проблем становится распространение дискредитирующей информации, подрывающей доверие к организациям, социальным институтам, отдельным лицам.

Отсутствие четкой системы выявления, анализа и предотвращения угроз дискредитации существенно увеличивает вероятность информационных атак на вышеуказанные объекты. В этом контексте создание математических моделей и разработка методов анализа признаков дискредитации сотрудников, основанных на данных из открытых источников, становится не просто актуальными, но и крайне важными задачами.

Необходимость научного исследования указанной темы особенно заметна на фоне растущего числа информационных манипуляций, нацеленных на подрыв репутации объектов из государственных и коммерческих структур. Такие действия приводят к серьезным последствиям не только локального, но и глобального характера, сказываясь на политиче-

ской, экономической и социальной стабильности как отдельных групп социума, так и общества в целом [2].

Дискредитирующие воздействия в Сети

В современном мире воздействие на общественное сознание и умы отдельных индивидов становится важнейшим фактором, определяющим работу организаций и их сотрудников. Дискредитация, как социальное явление, проявляется в различных формах – от банальной клеветы до манипуляций общественным мнением, нанося значительный ущерб отдельным личностям и целым организациям.

Дискредитация определяется как *преднамеренный и целенаправленный подрыв доверия к организации или отдельному индивиду путем распространения негативной, искаженной или ложной информации о них.*

Таким образом, основные формы дискредитации проявляются в: клевете – осознанном распространении недостоверных сведений об определенном объекте; искажении фактов – намеренной манипуляцией информацией для создания негативного восприятия того или иного объекта; фейковых новостях – вымышленных событиях и фактах, распространяемых в СМИ; ассоциации с негативным контекстом – связывании объекта с нежелательными идеями или персонажами [3].

Необходимо отметить, что термин «социальный» в контексте настоящей статьи обозначает принадлежность к обществу и взаимодействие между людьми, в то время как «медиа» подразумевает средство передачи информации в обществе. Объединяя эти понятия, термин «социальные медиа» можно определить как платформы, через которые люди делятся информацией, выражают мнения и обсуждают различные события или явления, происходящие в их жизнедеятельности.

Социальные медиа (СМ) выступают как интерактивные платформы, созданные для упрощения коммуникации между частными пользователями, организациями и корпорациями. СМ постепенно вытесняют традиционные методы маркетинга и становятся неотъемлемым инструментом продвижения товаров и услуг, активно способствуют продвижению концепции «узнаваемости бренда».

СМ обеспечивают возможность обмена идеями, фотографиями и видеоматериалами, что делает их важным компонентом современных маркетинговых стратегий в широком плане, но одновременно открывают нишу для противодействия таким стратегиям со стороны конкурента, противника, да и просто завистника, к чужому успеху, достижению, путем дискредитации последних.

Ключевыми составляющими дискредитирующих действий выступают три системно взаимосвязанных элемента: социальное взаимодействие, контент и коммуникационные средства. Эти три элемента формируют инфокоммуникационную основу в виде СМ для реализации дискредитирующих воздействий (Рис. 1).

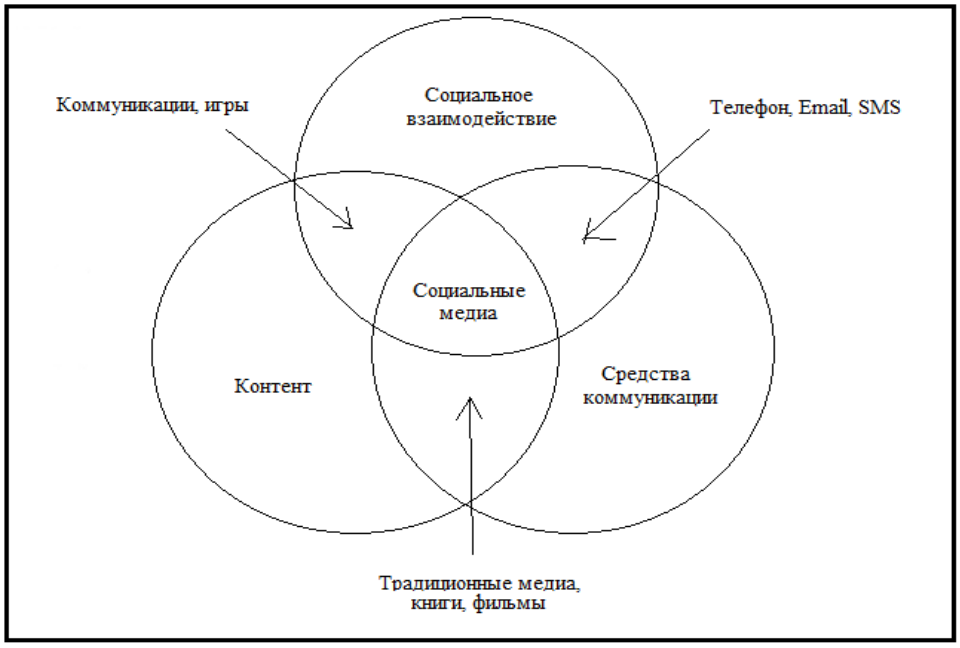

Рис. 1. Социальные медиа в системе реализации дискредитирующих воздействий

Очевидно, что для успешного функционирования всех представленных компонентов в «системе» дискредитации, если хотите так величать в целом это негативное явление, они должны быть интегрированы и доступны в нужное время. Раскроем кратко их содержание.

Социальное взаимодействие предполагает установление и развитие связей между пользователями социальных медиа через платформы.

Контент – это данные, доступные в социальных медиа, способные привлечь внимание аудитории.

Коммуникационные средства выполняют функцию обмена информацией и ускорения взаимодействия.

В эпоху глобальной цифровизации СМ стали важнейшим инструментом общения, предоставляя доступ к информации, влияя на общество, индивида как на локальном, так и на глобальном уровнях.

СМ значительно изменили восприятие людьми окружающего мира, способы коммуникации и обмена мыслями. Их преимущества многогранны [4], включая:

1. *Анонимность* – можно скрывать свою личность, используя псевдонимы.
2. *Разнообразие* доступной информации.
3. *Публичное представление* жизнедеятельности.
4. *Оперативность распространения* информации.
5. *Формирование* новых социальных связей.
6. *Субъективность воздействия*, вытесняющая объективность в восприятии данных.
7. *Изменение форматов* представления информации, включая трансформацию текстов, изображений и видеоматериалов.

8. *Запаздывание цензурирования*, не успевающего за скоростью информационных изменений.

Роль медийных платформ в системе дискредитации

Медийные платформы представляют собой сложные структуры, объединяющие частных лиц и организации посредством реализации своих социально-экономических, эмоциональных и финансовых отношений и связей. СМ выступают каналом коммуникации, связывающим людей, которые демонстрируют множество моделей поведения. В рамках исследований авторов изучаются вопросы математического моделирования распространения дискредитирующей информации.

Сегодня СМ являются основой распространения дискредитирующей информации в мировом киберпространстве. Примеры подобного рода можно встретить в разных странах. Так, в США дискредитация политиков и бизнесменов стала частью повседневной реальности, особенно в период избирательных кампаний.

СМ используются для распространения недостоверных сведений о кандидатах, серьезно влияя на имидж и их общественное восприятие. Например, в ходе президентской кампании 2016 года против Хиллари Клинтон проведена масштабная кампания, включавшая публикацию ложной информации о ее здоровье и использовании личного сервера электронной почты [5]. Эти действия заметно ухудшили ее репутацию в глазах избирателей.

Дональд Трамп также подвергся атакам, включая обвинения в связях с Россией, что, в конечном итоге, повлияло на выборную компанию и на общественное мнение в период его президентства [6].

В Европе дискредитация становится все более распространенным явлением, особенно в деловой сфере. В Германии компании сталкиваются с атаками на своих руководителей, когда конкуренты используют компрометирующую информацию для снижения доверия. Это негативно сказывается на моральном состоянии сотрудников, финансовом положении компаний и их репутации. Яркий пример – скандал с Volkswagen в 2015 году, приведший к значительным финансовым потерям и серьезному удару по репутации компании на международной арене [7].

На корпоративном уровне дискредитация ухудшает атмосферу в коллективе. А именно, сотрудники, ставшие мишенью информационных атак, часто чувствуют изоляцию и беспомощность, что снижает их мотивацию к продуктивному труду.

В Японии такие случаи уже приводили к массовым увольнениям персонала и утрате доверия к компаниям. Например, скандал вокруг Kobe Steel в 2017 году, связанный с подделкой сертификатов качества, подорвал репутацию фирмы, привел к падению стоимости акций [8].

Дискредитация негативно влияет на отношения организаций с клиентами. Она снижает доверие со стороны клиентов, что влечет за собой финансовые потери. Очевидно, что для минимизации такого рода рисков

необходимо активно работать над развитием положительного имиджа компании, укреплять внутренние коммуникации и развивать культуру доверия в ней. При этом обучение сотрудников медиаграмотности становится важным фактором в защите от информационных манипуляций в их отношении и сохранения репутации компании.

Современные возможности киберпространства предоставляют злоумышленникам мощные инструменты для манипуляции общественным мнением. Социальные сети и мессенджеры, информационные платформы для обмена контентом, различные форумы создают условия для стремительного распространения искажённой или ложной информации. Специальные алгоритмы, управляющие контентом, усиливают влияние провокационных или эмоциональных негативно насыщенных публикаций, позволяя дискредитирующим материалам быстро становиться вирусными.

Особую роль в этом процессе играют технологии ботов и фейковых аккаунтов, активно использующихся для создания искусственной популярности дискредитирующего контента. Эти технологии помогают создавать иллюзию широкой общественной поддержки, усиливая влияние манипулятивной информации на аудиторию.

Распространение ложной информации нередко остается безнаказанным, поскольку многие не проверяют ее достоверность. Важную роль в этом играют популярные блогеры и медийные личности, которые формируют удобные нарративы для ими же формируемых целевых общественных групп. Используя возможности социальных сетей, видеоплатформ и подкастов, они создают специализированный контент, насыщенный эмоциями, который, благодаря алгоритмам цифровых платформ, стремительно набирает популярность. В результате формируются новые медиа-системы, способствующие усилению и ускорению распространения дискредитирующей информации.

Технологические особенности медийного воздействия

Создание современных медиа-систем – процесс сложный, обусловленный взаимодействием целого ряда факторов. Важнейшим из них выступают алгоритмы, управляющие распределением контента в СМ. Такие алгоритмы ориентированы на повышение вовлеченности пользователей в реальную или выдуманную ситуацию и активно продвигают информацию, вызывающую яркие эмоции – гнев, страх или восхищение. Именно поэтому эмоционально насыщенные материалы приобретают намного больший охват по сравнению с нейтральными сообщениями.

Доступность цифровых технологий открыла широкие возможности для участия в создании контента. Сегодня им занимаются не только профессиональные журналисты, но и блогеры, активисты и даже анонимные авторы. Этот процесс значительно снижает порог входа в информационное пространство, позволяя обойти устоявшиеся традиционные стандарты журналистики, включающих проверку достоверности данных.

Влияние новостных систем усиливается за счет взаимодействия различных информационных платформ. Материалы, появившиеся в одной из них, быстро распространяются на другие, создавая взаимоусиливающие циклы. Кроме того, алгоритмы помогают формировать узкие сообщества, где пользователи окружены информацией, соответствующей их убеждениям. Это создает иллюзию ее достоверности, подкрепленную поддержкой якобы единомышленников.

Конечно же, нельзя забывать и про коммерческую составляющую, связанную с тем, что лидеры мнений, представляющие те или иные платформы, заинтересованы в повышении охватов и вовлеченности пользователей, поскольку это напрямую влияет на их доходы от рекламы и спонсорских контрактов. При этом эмоционально насыщенные, скандальные темы становятся основным инструментом для привлечения внимания и удержания аудитории. Их контент часто более персонализирован, чем материалы традиционных медиа. Они делятся своими переживаниями, демонстрируют эмоции и активно взаимодействуют с подписчиками, формируя ощущение искренности.

Стоит отметить, что подчас скептическое отношение в определенных кругах населения к крупным медиакомпаниям также способствует популярности альтернативных источников информации. Многие воспринимают блогеров как непредвзятых комментаторов, которые несут правду, игнорируемую традиционными СМИ.

Медиа-системы, значительно изменив информационное пространство, в то же время стали катализатором распространения дискредитирующей информации. За счёт эмоциональной насыщенности и вирусности такие материалы усиливают поляризацию в обществе, углубляя разрыв между разными социальными группами, подрывая доверие к официальным источникам информации, усложняя борьбу с манипулятивными данными.

Современные лидеры мнений и создаваемые ими новостные системы оказывая колоссальное воздействие на восприятие информации и формирование общественного мнения, активно участвуют в формировании и управлении восприятием событий. Поэтому понимание механизмов их деятельности и факторов, способствующих их популярности, является необходимым шагом для разработки моделей и методов противодействия манипуляциям и предотвращения распространения дискредитирующей информации в киберпространстве. Ясно, что только технологически подкреплённый подход способен противостоять нарастающей в нем информационной нестабильности в условиях нарастающей неопределённости и угроз.

Для противодействия возникшим вызовам требуется применение современных технологий, таких как большие данные, нейронные сети, инструменты визуализации данных.

Большие данные (Big Data) представляют собой структурированные и неструктурированные массивы данных большого объёма, а также современные автоматизированные инструменты их обработки для последующе-

го применения полученных результатов для анализа, прогнозирования и принятия управленческих решений.

Нейронные сети предоставляют возможность поиска смысла текстов, аудио- и видео информации, включая выявление манипулятивных воздействий на человека, например, DeepFake, или других форм информационных искажений.

Визуализация данных отображает взаимосвязи между ключевыми фигурами, событиями и организационными структурами, делая анализ более понятным и наглядным, обеспечивая эффективные стратегий для управления ситуацией.

Заключение

В заключение, говоря детально о технологиях комплексного анализа содержимого Сети при поиске информации дискредитирующего характера, рассмотрим наиболее эффективные на сегодняшний день инструменты:

Для анализа текстов с целью обнаружения манипулятивных технологий, включая DeepFake и другие формы искажений, предлагается, на наш взгляд, наиболее точная нейронная сеть BERT (Bidirectional Encoder Representations from Transformers) и ее производные [9; 10]. Она активно используется для задач классификации текста, анализа тональности, обнаружения фейковых новостей и манипулятивных текстов.

При аудиальном анализе применяются модели типа Wav2Vec 2.0 и OpenAI Whisper для расшифровки речи и выявления манипулятивной интонации. Для анализа видео используются EfficientNet, XceptionNet и MesoNet, которые показывают высокую результативность в обнаружении визуальных манипуляций. Обучение названных моделей производится на специализированных наборах данных: для текста – LIAR (корпус фейковых новостей) и PAN datasets, для аудио – VoxCeleb и Librispeech, а для видео – DeepFake Detection Challenge (DFDC) и FaceForensics++.

Для автоматизированного извлечения данных в социальных сетях среди наиболее эффективных инструментов иностранного происхождения можно выделить PhantomBuster и Octoparse, а также Netlytic, используемые для анализа текстов и связей между пользователями. Для интеграции с Twitter используется специализированная библиотека Tweepy, с Facebook – Facebook Graph API, для общего веб-скрейпинга – Scrapy. Для анализа сложных динамических страниц и создания парсеров, способных работать с закрытыми группами, эффективен инструмент Selenium. Библиотека BeautifulSoup применяется для обработки HTML-структур, что делает её удобной для работы с контентом, собранным из нестандартных источников.

При работе с социальными сетями и мессенджерами в России эффективно применяются отечественные разработки, такие как поисковая система SEUS – программный комплекс для мониторинга, поиска и анализа информации. Применяется для развития безопасного информационного

пространства и защиты российского общества от деструктивного информационно-психологического воздействия.

Интеграция рассмотренных в статье подходов и технологий позволит не только эффективно выявлять и предотвращать угрозы дискредитирующих воздействий в обществе, но и создавать условия для противостояния их распространению в социальных медиа. В условиях роста информационных вызовов и усложнения цифровых систем такие подходы становятся незаменимыми инструментами для защиты репутации, обеспечения доверия к медиа информации.

Список литературы

1. Минаев В.А., Бондарь К.М., Рабчевский А.Н., Федорович В.Ю. Противодействие экстремистской идеологии в социальных медиа: математические модели и методы: Монография / Под ред. В.А. Минаева, К.М. Бондаря. – Хабаровск: РИО ДВЮИ МВД России, 2023. – 232 с.

2. Бондаренко Е.Н., Анализ речевой стратегии дискредитации в лингвистической экспертизе (на примере интернет-комментария). // Филологические науки. Вопросы теории и практики. 2014. № 10 (40). Часть 1. – С. 27-29. EDN: SODFJZ

3. Кихтан В.В., Мамиева Б.Ю. К вопросу о манипулировании в современных СМИ // Вестник Волжского университета имени В. Н. Татищева. 2018. № 2. URL: https://cyberleninka.ru/article/n/k-voprosu-o-manipulirovanii-v-sovremennyh-smi (Дата обращения: 15.12.2024). EDN: XREBMT

4. Васильев Э.А., Дьяченко Н.Н. Субъекты дискредитации сотрудников органов внутренних дел // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2019. № 4 (48). – С. 56—60. DOI: 10.36511/2078-5356-2019-4-56-60 EDN: JEHXWY

5. Президентская кампания Хиллари Клинтон (2016). URL: https://ru.wikipedia.org/wiki/Президентская_кампания_Хиллари_Клинтон_(2016). (Дата обращения 15.12.2024).

6. Federal Prosecution of Donald Trump (classified documents case). URL: https://translated.turbopages.org/proxy_u/en-ru.ru.0a3a3912-675aaa2f-5458b0cc-74722d776562/https/en.wikipedia.org/wiki/Federal_prosecution_of_Donald_Trump_(classified_documents_case). (Дата обращения 15.12.2024)

7. Volkswagen Emissions Scandal.URL: https://translated.turbopages.org/proxy_u/en-ru.ru.3f92f82e-675aaa84-1539d6c8-74722d776562/https/en.wikipedia.org/wiki/Volkswagen_emissions_scandal. (Дата обращения 15.12.2024)

8. Kobe Steel. URL: https://en.m.wikipedia.org/wiki/Kobe_Steel. (Дата обращения 15.12.2024).

9. Минаев В.А., Поликарпов Е.С., Симонов А.В. Применение глубинных нейронных сетей для выявления деструктивного контента в соци-

альных медиа // Информация и безопасность. 2021. Т. 24. № 3. – С. 361-372. DOI: 10.36622/VSTU.2021.24.3.004 EDN: IMHBIG

10. Минаев В.А., Симонов А.В. «Просеивание» телеграмм-каналов при поиске контента экстремистского характера // Информация и безопасность: научный журнал. 2023. Том 26. № 1. – С. 25-30.

IDENTIFYING DEFAMATORY INFORMATION IN CYBERSPACE: MODERN FEATURES

V.A. Minaev, A.S. Kolomina
Moscow University named after V. Ya. Kikot

Abstract. The issues of identifying, analyzing and preventing threats to discredit organizations and specific individuals using social media are considered. Attention is drawn to the use of mathematical methods and models in describing the processes of defamatory information propagation. The definition is given, the main forms are discussed and examples of discrediting are given. The role of social media in the system of discrediting effects is shown. It is concluded that in the context of increasing information challenges and the complexity of digital applications, the considered methods and models are becoming indispensable tools for protecting reputation and ensuring trust in media information.
Keywords: *discredit threats, social media, discrediting information, discrediting influences.*

СИСТЕМА ВЫЯВЛЕНИЯ ИНФОРМАЦИОННЫХ АТАК

Я.Р. Мустакимова, А.Н. Рабчевский
Пермский государственный национальный исследовательский университет

Аннотация. Данная статья посвящена системе автоматического выявления информационных атак в социальных сетях. В системе анализируются следующие признаки информационных атак: использование ботов для распространения информации, распространение четких и нечетких дубликатов сообщений, использование независимых каналов распространения информации. Целью работы является создание комплексного подхода к мониторингу и анализу информационных потоков в социальных сетях, что поможет в своевременном обнаружении и противодействии информационным атакам.
Ключевые слова: *информационные атаки, методы обнаружения информационных атак, социальные сети, боты, четкие и нечеткие дубликаты, независимые каналы.*

Введение

В наши дни социальные сети играют важную роль, они стали одним из основных способов общения и взаимодействия людей. Популярность социальных сетей непрерывно растет, что объясняется простотой их использования и широкой доступностью. Социальные платформы предоставляют возможность быстро находить интересных собеседников, делиться опытом, а также получать актуальную информацию и развлекательный контент. Тем не менее, с увеличением популярности социальных сетей увеличиваются и риски, связанные с их использованием. К сожалению, эти платформы часто привлекают злоумышленников, которые используют социальные сети для деструктивного влияния на общественное мнение. Злоумышленники активно распространяют ложную информацию через социальные сети, провоцируют конфликты, что в свою очередь приводит к росту социальной напряженности в обществе. Таким образом злоумышленники используют социальные сети для проведения информационных атак. Чтобы предотвратить такие атаки, их сначала нужно обнаружить. Создание методов, алгоритмов и программных решений для этой цели является крайне важной и актуальной задачей.

Обзор литературы

Информационная атака – это спланированное, организованное, целенаправленное, массированное информационное воздействие на объекты с целью формирования общественного мнения и поведения в соответствии с задачами организаторов атаки [1].

Существует множество различных объектов, на которые оказывают влияние информационные атаки. Целью информационных атак может быть общество в целом. Здесь речь идет о гражданах, которые становятся жертвами дезинформации, распространяемой в социальных сетях. Чаще всего такие атаки нацелены на создание паники, внушение страха или же изменение общественного мнения по вопросам, касающимся политики, экологии, безопасности или других актуальных тем. Массовая дезинформация может приводить к протестам и серьезным общественным беспорядкам. Также объектами информационных атак являются государственные институты. Злоумышленники могут пытаться подорвать репутацию конкретных лидеров или партий, распространяя недостоверную информацию. Не следует забывать и о специфических группах и сообществах. Это могут быть этнические или религиозные меньшинства, а также любые другие группы с определенной социальной идентичностью. Атаки на них могут быть направлены на разжигание ненависти, подстрекательство к дискриминации и насилию, на создание ложных стереотипов.

Если информационная атака достигла своих первоначальных целей, будь то изменение общественного мнения, манипуляция выборами, подрыв доверия к определенным личностям и организациям, или создание беспорядка в обществе, то она считается успешно проведенной.

Типовая информационная атака в социальных сетях проводится в два этапа. Первый этап – это вброс информации. Под информационным вбросом понимается резкое заполнение сетевого пространства какой-либо короткой, вызывающей массу эмоций информацией [2]. В социальных сетях этап вброса происходит через публикацию постов на страницах пользователей и в сообществах, причем публикацию могут осуществлять как реальные аккаунты, так и автоматизированные боты. Второй этап – это разгон контента. Он подразумевает реакцию на уже размещенные посты, включая репосты или комментарии. Пользователь может выразить свое одобрение через лайки или просто ознакомиться с постом. Все эти действия имеют значительное влияние на распространение информации. Обнаружение информационной атаки на этапе вброса значительно ускоряет реакцию на неё и позволяет осуществить противодействие на самом начальном этапе, предотвращая достижение целей злоумышленника.

Идея о выявлении информационных атак не нова. Существует два основных подхода к ее реализации [3]:

1. Классический метод. Этот метод заключается в анализе количества сообщений определенной направленности в пределах заданного времени. Превышение количества сообщений над пороговым значением является свидетельством проведения информационной атаки.

2. Метод, основанный на анализе динамики информационных потоков. Этот метод включает в себя построение графика изменения объема публикуемых сообщений и его сопоставление с заранее заданным шаблоном. Если графики совпадают, то это указывает на наличие информационной атаки.

Недостатком данных методов является то, что они не способны оперативно выявлять информационные атаки, поскольку требуется анализ публикуемых сообщений за достаточно длительный срок.

Анализируя общедоступные источники, можно заметить, что исследователи применяют различные сочетания признаков для выявления информационных атак. Среди этих признаков можно выделить: публикация схожего по содержанию целевого контента и высокая частота таких публикаций [3], небольшой временной интервал между публикациями [4], значимость источника и стремление к максимальному охвату аудитории [5] и др. Также уже существует патент «Система и способ выявления информационной атаки», автор – Нежданов Игорь Юрьевич [6]. В данном патенте представлено изобретение, которое позволяет автоматически выявлять факты проведения информационных атак и незамедлительно уведомлять ответственных лиц о таких атаках. Описанная в патенте система направлена на анализ различных интернет-ресурсов, таких как новостные сайты, блоги, форумы, видеохостинги, стриминговые платформы и сервисы вопросов и ответов. Для определения факта информационной атаки исследуются следующие параметры: общее число публикаций; количество сообщений, размещенных ботами, и количество управляемых ботами аккаунтов; количество публикаций, отправленных группами связанных источников; общее число дублирующихся публикаций.

Нашей же задачей является разработка системы автоматического выявления информационных атак в социальных сетях.

Система выявления информационных атак

В предлагаемой нами системе планируется использовать следующие признаки информационных атак:

1. Использование ботов для распространения информации. До сих пор не выработано однозначное определение термина «бот социальной сети». Мы будем рассматривать бот как специализированную страницу (аккаунт) в социальной сети, которая имитирует обычного пользователя и автоматически выполняет действия по публикации и продвижению контента для достижения целей злоумышленников.

2. Распространение четких и нечетких дубликатов сообщений. Четкий дубликат – это сообщение, которое точно совпадает с исходным сообщением по содержанию, формату и другим критериям. Например, если два сообщения полностью идентичны (одинаковый текст, изображения, ссылки), они считаются четкими дубликатами. Обычно такие дубликаты легко обнаруживаются с помощью алгоритмов сравнения текстов. А нечеткий дубликат – это сообщение, которое не является идентичным исходному сообщению, но имеет значительное совпадение по содержанию или смыслу. Нечеткие дубликаты могут включать небольшие переработки текста, изменения в формулировках или в порядке представления информации. Например, публикации, говорящие об одном и том же событии, но с разной формулировкой, могут считаться нечеткими дубликатами. Обнару-

жить нечеткие дубликаты намного сложнее, поэтому злоумышленники могут использовать их при проведении информационных атак.

3. Использование независимых каналов распространения информации. Под независимыми каналами в данном контексте подразумеваются аккаунты в социальных сетях, которые не имеют связей друг с другом. Вероятность того, что множество незнакомых людей станет одновременно публиковать одинаковый контент без общей цели, крайне мала. Такое поведение свидетельствует об организованной деятельности тех, кто инициирует информационную атаку.

Мы считаем, что именно эти признаки позволят нам обнаружить информационные атаки на ранней стадии. Архитектура нашей системы представлена на рисунке.

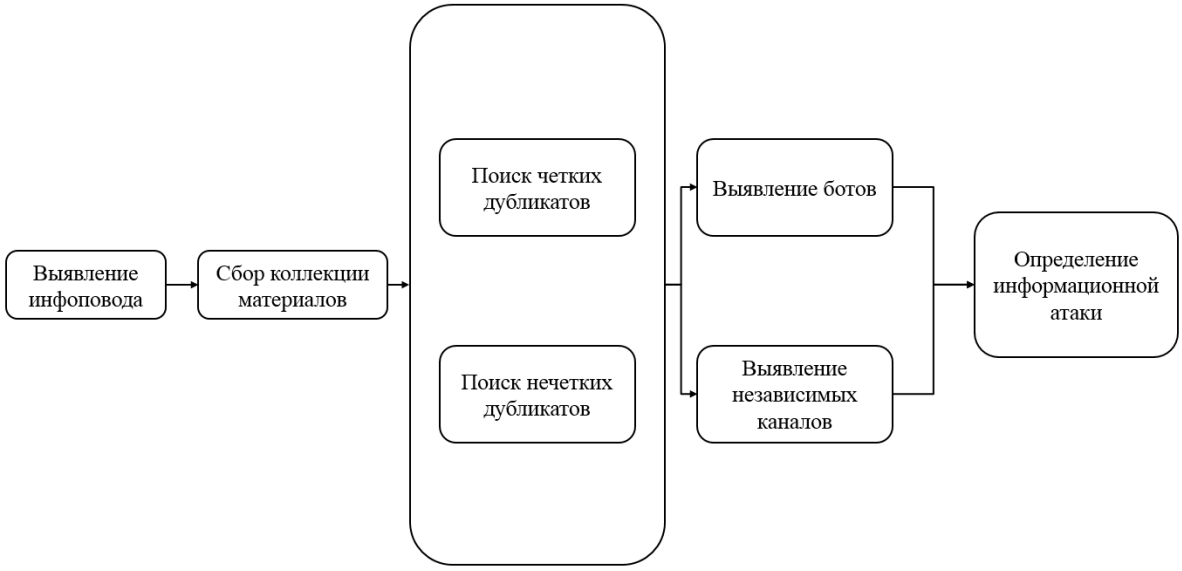

Рис. Архитектура системы автоматического выявления информационных атак в социальных сетях

Процесс работы нашей системы можно представить в виде следующей последовательности действий:

1. Выявление инфоповода. Инфоповод – это серия сообщений, публикуемых пользователями в социальных сетях, объединенных определенной тематикой. Инфоповод может быть связан с обсуждением какого-нибудь события, новости или темы, которая интересует большое количество людей в данное время. Инфоповоды могут быть как положительными, когда, например, обсуждается значимое событие или достижение, вдохновляющее людей и вызывающее одобрение, так и негативными. Такие темы, как коррупционные скандалы или социальные проблемы, тоже часто привлекают внимание людей и становятся предметом активных обсуждений в социальных сетях.

2. Сбор коллекции материалов. На данном шаге происходит сбор сообщений, которые относятся к выбранному информационному поводу. При этом собираются все сообщения, а не только те, которые имеют нега-

тивный характер. Потому что сообщения нейтрального и позитивного характера также могут быть частью информационных атак.

3. Формирование информационных треков. Информационный трек можно рассматривать как поток сообщений, созданных пользователями социальных сетей, состоящий из повторяющихся записей, упорядоченных по времени. Информационная атака, как правило, включает множество таких треков. В начале запуска трека контент распространяется быстро и в большом объеме от разных аккаунтов, что приводит к массовому вбросу информации. На данном шаге отдельно формируются треки с четкими и нечеткими дубликатами. Для работы с четкими дубликатами разработана и зарегистрирована программа «Информационный трек-детектор» [7], которая выявляет в общем потоке сообщений четкие дубликаты. Для выявление нечетких дубликатов также разработана и зарегистрирована программа «Программа выявления нечетких текстовых дубликатов» [8]. Процесс выявления нечетких дубликатов состоит из двух этапов: векторизация и кластеризации полученных векторов. Для векторизации была выбрана модель Transformers [9] – это архитектура нейронной сети, которая получила широкое применение в области обработки естественного языка (Natural Language Processing, NLP). Для кластеризации был выбран метод DBSCAN (Density-based spatial clustering of applications with noise, плотностной алгоритм пространственной кластеризации с присутствием шума) [10], который как следует из названия, оперирует плотностью данных.

4. Выявление ботов. Для обнаружения ботов разработана и зарегистрирована программа «Детектор ботов» [11]. На основе обученных нейросетевых моделей программа классифицирует профили пользователей социальной сети на две категории – «Боты» и «Не боты». В процессе исследования рассматриваются как открытые, так и закрытые профили пользователей.

5. Выявление независимых каналов. Для выявления независимых каналов разработана программа, которая определяет связи между аккаунтами, то есть ищет общих друзей, и на основе полученной информации строит граф связей.

Таким образом, анализируя динамику распространения дубликатов вместе с выявлением ботов и независимых каналов, можно установить факт проведения информационной атаки.

Заключение

Для разработки надежной и статистически обоснованной системы необходимо провести углубленное исследование разнообразных информационных атак. Ключевую роль в системе играют пороговые значения, такие как количество необходимых сообщений для формирования информационных треков или минимальный процент ботов среди участвующих аккаунтов. Эти пороговые значения помогут в принятии обоснованных решений относительно факта проведения информационной атаки. Важно понимать, что различные сценарии атак могут требовать различных порого-

вых значений, что подчеркивает необходимость дальнейших исследований в этой области. Установление и уточнение этих значений станет основой для более эффективного мониторинга и реагирования на угрозы, исходящие из информационного пространства.

Список литературы

1. Коцюбинская Л.В. Информационная атака: понятие и онтологические свойства // Политическая лингвистика. 2017. №6. С. 106-111. EDN: YMJXMA
2. Кочешев П.А. Информационные «вбросы». Методы минимизации последствий // Проблемы науки. 2016. № 6(7). С. 24-25. EDN: WDFTFZ
3. Потемкин А.В. Распознавание информационных операций средств массовой информации сети Интернет // Интернет-журнал «Науковедение». 2015. Т. 7. № 3. С. 1-11. DOI: 10.15862/139TVN315 EDN: UMFXXB
4. Еременко В.Т. Информационное противоборство в социотехнических системах / В. Т. Еременко, П. Н. Рязанцев. Орел: ОГУ имени И.С. Тургенева, 2016. 209 с. EDN: ZBYMMP
5. Расторгуев С.П. Информационные операции в сети Интернет / С. П. Расторгуев, М. В. Литвиненко, под. общ. ред. А. Б. Михайловского. Москва: АНО ЦСОиП, 2014. 128 с. ISBN: 978-5-906661-05-0 EDN: YNDAPK
6. Нежданов И.Ю. Система и способ выявления информационной атаки [Электронный ресурс] URL: https://www.fips.ru/registers-doc-view/fips_servlet?DB=RUPAT&DocNumber=2789629&TypeFile=html (дата обращения: 07.12.2024)
7. Программа «Информационный трек-детектор» свидетельство о регистрации программы для ЭВМ регистрационный № 2022668598 от 10.10.2022.
8. «Программа выявления нечетких текстовых дубликатов» свидетельство о регистрации программы для ЭВМ регистрационный № 2024665993 от 09.07.2024.
9. Sentence transformers. Distiluse-base-multilingual-cased-v. [Электронный ресурс] URL: https://huggingface.co/sentence-transformers/distiluse-base-multilingual-cased-v1(дата обращения: 07.12.2024)
10. DBSCAN [Электронный ресурс] URL: https://scikit-learn.org/1.5/modules/generated/sklearn.cluster.DBSCAN.html (дата обращения: 07.12.2024)
11. Программа «Детектор ботов» свидетельство о регистрации программы для ЭВМ регистрационный № 2024617353 от 01.04.2024.

INFORMATION ATTACK DETECTION SYSTEM

Y.R. Mustakimova, A.N. Rabchevsky
Perm State University

Abstract. This paper is devoted to the system of automatic detection of information attacks in social networks. The system analyzes the following attributes of information attacks: the use of bots to disseminate information, the dissemination of clear and fuzzy duplicates of messages, the use of independent channels of information dissemination. The purpose of the work is to create a comprehensive approach to monitoring and analyzing information flows in social networks, which will help in the timely detection and counteraction to information attacks.
Keywords: *information attacks, information attack detection methods, social networks, bots, clear and fuzzy duplicates, independent channels.*

ДЕТЕКТИРОВАНИЕ БОТОВ В СОЦИАЛЬНЫХ СЕТЯХ

С.В. Брызгалов, Я.Р. Мустакимова, А.Н. Рабчевский
Пермский государственный национальный исследовательский университет

Аннотация. В статье рассматривается проблема применения ботов в социальных сетях, которые все чаще используются как средства для осуществления информационных атак. Целью данной работы является анализ текущего состояния методов выявления и противодействия ботам, а также разработка программы для их детектирования. С помощью разработанной программы был проведен анализ нескольких информационных атак, проведенных в социальной сети ВКонтакте. В результате проведенных исследований был сделан вывод о том, что мониторинг активности ботов может служить важным индикатором для идентификации новых информационных атак.
Ключевые слова: *информационные атаки, социальные сети, боты, детектирование ботов.*

Введение

В последнее время социальные сети стали неотъемлемой частью нашей повседневной жизни. Миллионы людей по всему миру пользуются ими для общения, обмена информацией и поиска развлекательного контента. С увеличением аудитории социальных сетей возникла потребность в автоматизации процесса управления контентом, что привело к популярности ботов.

В общем случае под ботом понимается программа, автоматически выполняющая заранее настроенные повторяющиеся задачи [1]. Боты обычно либо имитируют поведение пользователя, либо полностью заменяют его. В социальных сетях боты могут использоваться для различных целей. Например, с помощью ботов можно эффективно распространять информацию. Боты могут автоматически публиковать новости и объявления. Многие компании используют ботов для проведения рекламных кампаний, анализа пользовательских данных и формирования рекомендаций на основе поведения пользователей. Боты могут вести беседы с пользователями, предоставлять информацию о каких-либо продуктах или услугах.

Но также боты могут представлять собой серьезную угрозу. Некоторые боты специально создаются злоумышленниками для распространения фейковых новостей и манипуляции общественным мнением. Например, во время пандемии коронавируса боты в Twitter подвергали сомнению правдивость информации, распространяемой через официальные источники, и массово рассылали ссылки на недостоверные источники информации. Также боты распространяли посты с критикой мер, принятых для сдерживания пандемии [2]. Еще боты в социальных сетях могут использоваться

для шантажа или кражи личной информации [3]. В работе [4] отмечается, что вредоносные боты являются одним из основных инструментов проведения атак в социальных сетях.

Но несмотря на существенный прогресс в развитии методик выявления и противодействия ботам, методы определения характеристик ботов на данный момент развиты недостаточно. Боты не просто используются в информационных атаках, но и постоянно эволюционируют, что в свою очередь влияет на возможности их детектирования. Поэтому важно разрабатывать и совершенствовать средства, позволяющие отличить настоящих пользователей от ботов.

Обзор литературы

Согласно оценке компании Arkose Labs, 73% всего интернет-трафика в настоящее время составляют и распространяют боты [5]. Конечно, некоторые боты выполняют полезные функции, но большинство созданы для вредоносных целей.

Боты способны выполнять тысячи задач одновременно, что позволяет злоумышленникам не только экономить время, но и значительно увеличивать масштаб своих операций. С помощью ботов можно маскировать свое истинное местоположение и личность, что усложняет работу правоохранительным органам по выявлению и задержанию преступников. С помощью ботов можно манипулировать эмоциями и поведением реальных пользователей социальных сетей. В исследовании [6] говорится, что даже незначительное количество ботов в онлайн-среде может существенно изменить восприятие и взгляды реальных пользователей. Это происходит благодаря тому, что боты способны создавать иллюзию массовой поддержки определенных мнений и позиций, что влияет на общественное мнение. Также работа ботов может способствовать формированию фильтров, что тоже является серьезной проблемой. Алгоритмы социальных сетей, предназначенные для персонализации контента, часто создают фильтр, в результате работы которого пользователи сталкиваются преимущественно с теми мнениями, которые совпадают с их собственными. Например, если пользователь активно взаимодействует с определенным видом контента или поддерживает определённые взгляды, то боты начнут подбирать и показывать ему больше информации в этом же ключе, игнорируя альтернативные точки зрения. Это создает искаженное восприятие реальности и ограничивает критическое мышление человека. По всем этим причинам злоумышленники используют ботов при проведении информационных атак.

Для детектирования ботов можно использовать следующие методы:

1. Метод «живой силой». В данном случае поиском ботов занимаются модераторы. Они ищут ботов на основе жалоб от пользователей. Модераторы исследуют профиль пользователя: обращают внимание на наличие неполной информации, на отсутствие фотографии, на одинаковые или общие темы в публикациях и комментариях. Также модераторы отслеживают

необычные шаблоны поведения пользователей. Например, слишком высокую активность пользователя или работу пользователя в круглосуточном режиме. Однако модератор может потерять концентрацию внимания в течение нескольких минут рутинной работы, в следствии чего он может с легкостью не увидеть какой-то критически важный параметр или наоборот, добавить что-то от себя, чем уменьшит точность предсказания. Также при увеличении количества пользователей социальных сетей необходимо нанимать большее число модераторов.

2. Анализ структуры социального графа. Данный метод заключается в построении социального графа и его дальнейшем анализе. Для этого используются различные алгоритмы поиска компонент сильной связности [7]. При изучении топологии графа необходимо обратить внимание на узлы с необычными характеристиками. Например, боты могут иметь значительное количество подписчиков и подписок. Или если аккаунт имеет множество связей с другими пользователями, но не взаимодействует с ними, то это может быть подозрительным. Также боты могут образовывать отдельные кластеры или взаимодействовать лишь с определёнными группами, отличающимися от большинства пользователей. К недостаткам данного метода можно отнести большие временные затраты на построение графа, а также низкую точность метода, потому что итоговые выводы формирует человек, который может ошибиться.

3. Метод машинного обучения. Данный метод позволяет свести к минимуму человеческий фактор и субъективизм, потому что алгоритмы опираются на данные и заранее заданные критерии, что снижает вероятность ошибок, связанных с персональным мнением или предвзятостью модератора.

Метод, использующий машинное обучение, включает в себя два основных подхода. Первый заключается в анализе контента, который публикует пользователь [8]. Здесь ключевым моментом является работа с текстами сообщений, изображениями и видео, которые могут содержать маркеры, указывающие на автоматизированное поведение. Этот подход особенно эффективен для социальных сетей, где контент имеет однородный характер, поскольку это упрощает процесс классификации и выявления аномалий. Второй подход основывается на изучении метаданных аккаунта пользователя. В данном случае анализируются такие данные, как имя владельца аккаунта, дата его создания, объем размещенных материалов, количество друзей и подписок и т.д. Одной из ключевых проблем данного подхода является выбор и извлечение релевантных признаков, поскольку для достижения высокой точности анализа важно правильно определить, какие характеристики будут наиболее информативными.

Конечно и у этого метода есть свои недостатки. Например, алгоритмы часто разрабатываются с учетом особенностей конкретных социальных сетей, что затрудняет использование одних и тех же программных решений для разных социальных платформ. Также возникает сложность со сбором качественных данных для обучения, так как часто используются не-

большие или плохо размеченные наборы данных. Тем не менее алгоритмы машинного обучения могут анализировать и обрабатывать огромные объемы данных непрерывно за небольшой промежуток времени, что позволяет быстро выявлять подозрительное поведение и обнаруживать ботов.

Программа для детектирования ботов

Целью нашей работы является создание программы, позволяющей выявлять ботов в социальной сети ВКонтакте. ВКонтакте – это одна из самых популярных социальных сетей в России и странах СНГ, обеспечивающая доступ к широкой и разнообразной аудитории. Пользователи сети могут легко делиться публикациями, фотографиями, видео и другими материалами, что способствует быстрому распространению информации. Платформа поддерживает различные форматы контента – текст, изображения, видео, аудио – позволяя обмениваться информацией в удобном для пользователей виде. Возможности комментирования, лайков и репостов позволяют пользователям взаимодействовать с контентом, что также способствует распространению информации. Именно поэтому эту социальную сеть злоумышленники очень часто используют в своих целях.

Рассматривая методы детектирования ботов, мы решили остановиться на методе машинного обучения, как наиболее простом и эффективном решении для анализа большого количества пользователей.

Просмотрев аккаунты пользователей ВКонтакте, мы выделили параметры, которые будут поданы на вход нейронной сети. В социальной сети ВКонтакте есть два вида профилей пользователей – открытые и закрытые. У открытых профилей доступно больше данных для анализа, чем у закрытых. У закрытых профилей возможно считать только те параметры, которые в таблице 1 выделены серым цветом, в то время как у открытых можно считать все представленные в таблице параметры.

Таблица

Параметры аккаунтов

Наличие галочки	Кол-во подписок	Ср. кол-во дней между постами	Ср. кол-во просмотров на постах	Кол-во видео
Есть ли имя в словаре имен	Дней с последнего захода	Отношение постов и репостов	Кол-во подписчиков	Кол-во аудио
Есть ли никнейм	Возраст аккаунта в днях	Кол-во постов с удаленными	Кол-во подписчиков в VK Клипы	Кол-во подарков
Полнота заполнения профиля	Кол-во постов на данный момент	Кол-во постов в день за последние 100 постов	Кол-во фото профиля	Кол-во групп
Кол-во друзей	Кол-во постов в день за время жизни аккаунта	Ср. кол-во комментариев на постах	Кол-во указаний на фото	Кол-во городов в группах
Кол-во «Интересных страниц»		Ср. кол-во лайков на постах	Кол-во фотоальбомов	Кол-во групп без аватарок

Разделение профилей на открытые и закрытые производится для более достоверного анализа. В связи с этим были созданы две разные нейросетевые модели – для поиска ботов среди открытых профилей и для поиска ботов среди закрытых профилей. Обе нейронные сети представляют собой многослойный персептрон с одним скрытым слоем и одним выходным нейроном, который дает нам число от 0 до 1, которое обозначает вероятность того, что данный аккаунт – бот.

В ходе разработки нейросетевых моделей была изучена значимость всех входных параметров. Самым низким значением обладает параметр «наличие галочки», максимальное значение имеет параметр «возраст аккаунта». В результате анализа стало ясно, что каждый параметр влияет на конечный результат, и избавление даже от самых незначительных может сказаться на точности.

Набор данных для обучения собирался вручную. Аккаунты ботов были получены благодаря сайту Ботнадзор [9]. В качестве обычных пользователей были взяты аккаунты из групп различных школ, университетов, подслушано разных городов.

Проверка полученных нейросетевых моделей на тестовых данных показала следующие результаты: для открытых профилей – 95% точности выявления ботов, для закрытых – 86%.

После успешного тестирования нейросетевых моделей была написана программа «Детектор ботов» [10]. Она классифицирует профили пользователей ВКонтакте на две категории – «Боты» и «Не боты». Работу программы можно представить в виде следующей последовательности шагов:

1. На первом шаге осуществляется формирование текстового файла с ссылками на профили пользователей. Таким образом, любые профили ВКонтакте можно проверить, записав их в файл и передав его программе.

2. На втором шаге проводится разделение всех профилей на три группы: «Открытые», «Закрытые» и «Удаленные». Принцип разделения профилей по категориям, следующий: программа через VK API [11] проверяет каждый отдельный профиль и смотрит к какой группе его отнести. Все профили из категории «Удаленные» определяются как боты. Проанализировать удаленный профиль и получить какие-либо данные относительно его владельца нельзя, а вероятность того, что профиль был удален самим пользователем значительно ниже, чем вероятность того, что модераторы ВКонтакте заметили подозрительную активность и заблокировали бота.

3. На третьем шаге происходит сбор данных о пользователях из групп «Открытые» и «Закрытые». Все данные, необходимые для определения параметров из таблицы 1, извлекаются с помощью VK API. Следует отметить, что программа собирает только данные профиля, не затрагивая публикации пользователя, кроме времени этих самых публикаций. Это сделано для оптимизации сбора данных, основываясь на следующей логи-

ке: если модель нейронной сети для открытых пользователей уже может классифицировать профили с 95% точностью, то добавление двух-трех процентов к точности от анализа публикаций не оправдают временные затраты на их обработку. А к закрытым профилям такое решение и вовсе не применимо, так как невозможно просмотреть публикации закрытых профилей.

Чтобы облегчить взаимодействие с VK API, были созданы специальные процедуры. Но эти процедуры накладывают некоторое ограничение на работу программы: списки профилей обрабатываются наборами размером не более 25 профилей в каждом. Данное решение обеспечивает некоторую степень сохранности от сбоев в работе программы. Если произойдет сбой, то потеряется только информация о последних 25 профилях. Информация о профилях, проанализированных ранее, сохранится.

4. На четвертом шаге осуществляется нейросетевой анализ. После сбора данных проводится их нормализация для того, чтобы ни один из параметров не был более важным просто потому, что он измеряется в десятках тысяч, а не в единицах. Все параметры должны быть равнозначными в возможностях своего влияния на итоговый результат. Параметры в данных проходят избавление от выбросов и нормализуются до значений от 0 до 1 с помощью метода скорректированного интервала, после чего подаются на вход нейросетевым моделям. На выходе мы получаем вероятность того, что проверяемый аккаунт является ботом. Для облегчения дальнейшей работы с этой информацией было принято решение считать все аккаунты, вероятность которых ниже 0.5 – «Не ботами», а те, у которых выше 0.5 – «Ботами».

Результаты

С помощью разработанной программы мы решили проверить как используются боты для проведения информационных атак в социальных сетях.

Мы проанализировали два информационных повода, по которым проводились информационные атаки в социальной сети ВКонтакте: «Дворец Путина» и «Специальная военная операция». Результаты показали, что для «Дворца Путина» в среднем 24% постов создаются ботами, тогда как для «Специальной военной операции» этот показатель значительно выше – 67%.

После чего нам стало интересно посмотреть, нет ли какой закономерности в том, когда используются боты. Мы предполагали обнаружить два теоретических шаблона (рис. 1). Первый – это постепенное уменьшение процента постов ботов со временем, когда реальные пользователи подхватывают сообщение и начинают распространять его сами. То есть людям становится интересна определенная информация и боты, как инструмент распространения, отходят на задний план. Нам показалось, что

это будет выглядеть более естественно с точки зрения распространения информации. Второй – это постепенное увеличение процента постов ботов от времени. В этом случае люди не проявляют интереса к определенной информации, не распространяют её самостоятельно, и эту задачу берут на себя боты. Ведь конечная цель информационной атаки – это довести нужную злоумышленнику информацию до обычных людей, а чем больше постов с этой информацией, тем выше шанс, что пользователи её увидят.

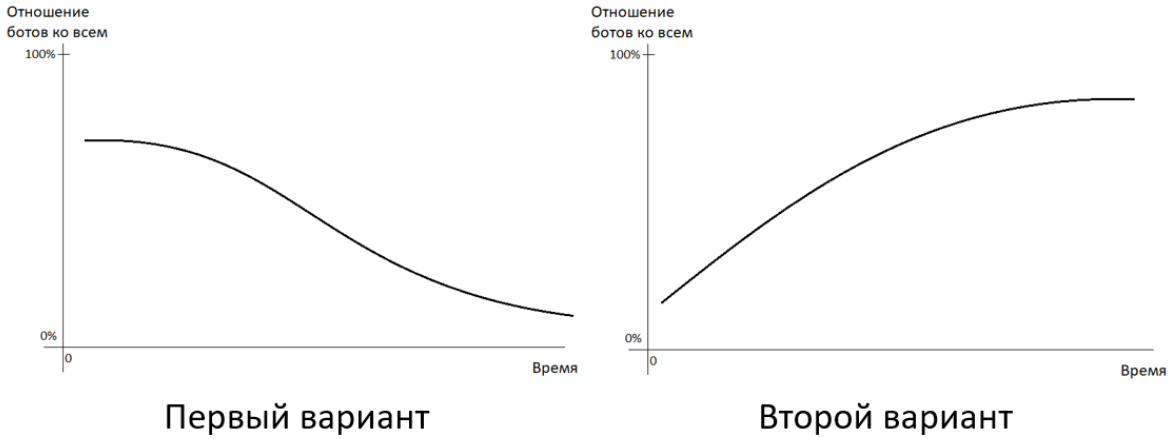

Рис. 1. Теоретические шаблоны

На практике мы получили следующие результаты. Во-первых, мы выявили случаи (рис. 2), когда пост сначала создавался и публиковался человеком, затем его начали распространять обычные пользователи, а позже к этому процессу подключились и боты. В таких случаях можно заметить, что соотношение постов, генерируемых ботами, к общему числу постов остается на постоянном уровне на протяжении всего времени.

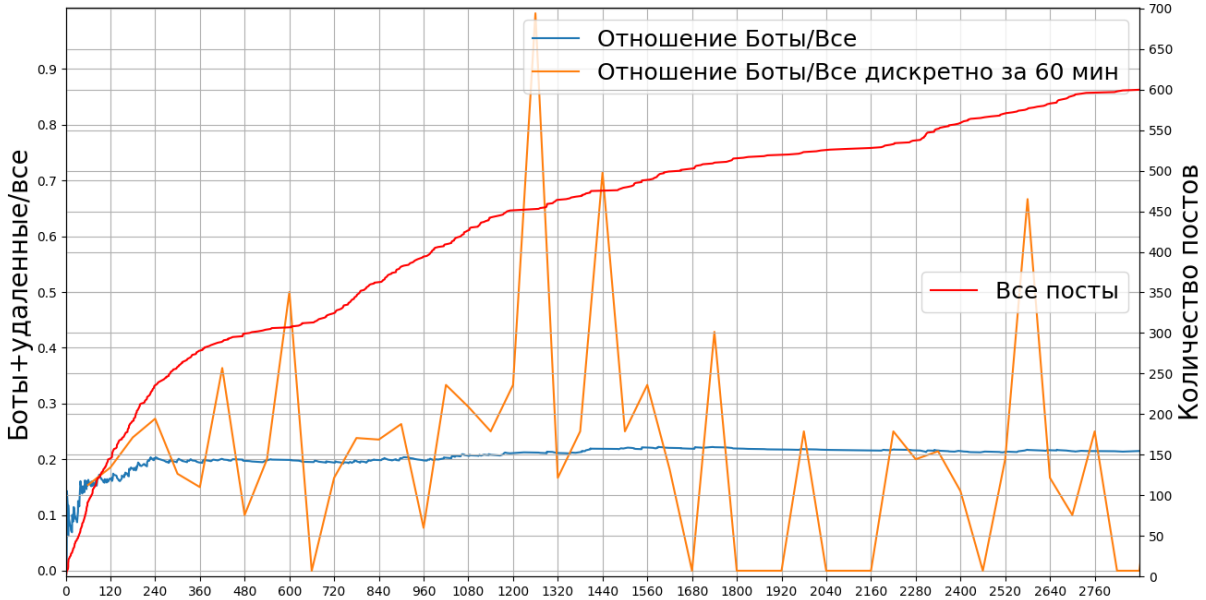

Рис. 2. Практический шаблон 1

Во-вторых, есть случаи (рис. 3), когда первые несколько постов публикуются ботами, а затем эти посты начинают распространять люди совместно с ботами.

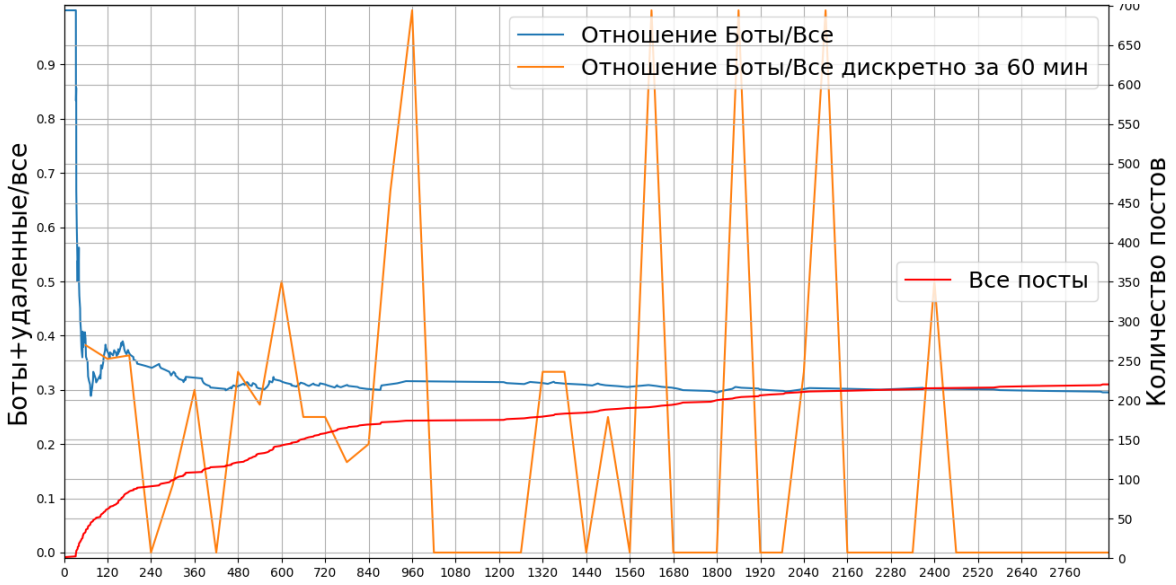

Рис. 3. Практический шаблон 2

По сути, оба этих случая подходят под первый теоретический шаблон, но вместо того чтобы снижать активность, боты продолжают свою работу.

Также мы выявили случаи (рис. 4), когда посты распространяют исключительно боты. Например, один и тот же пост боты размещали в нескольких группах в течении пары месяцев. Такие случаи вписываются во второй теоретический шаблон, когда сообщения преимущественно распространяются ботами.

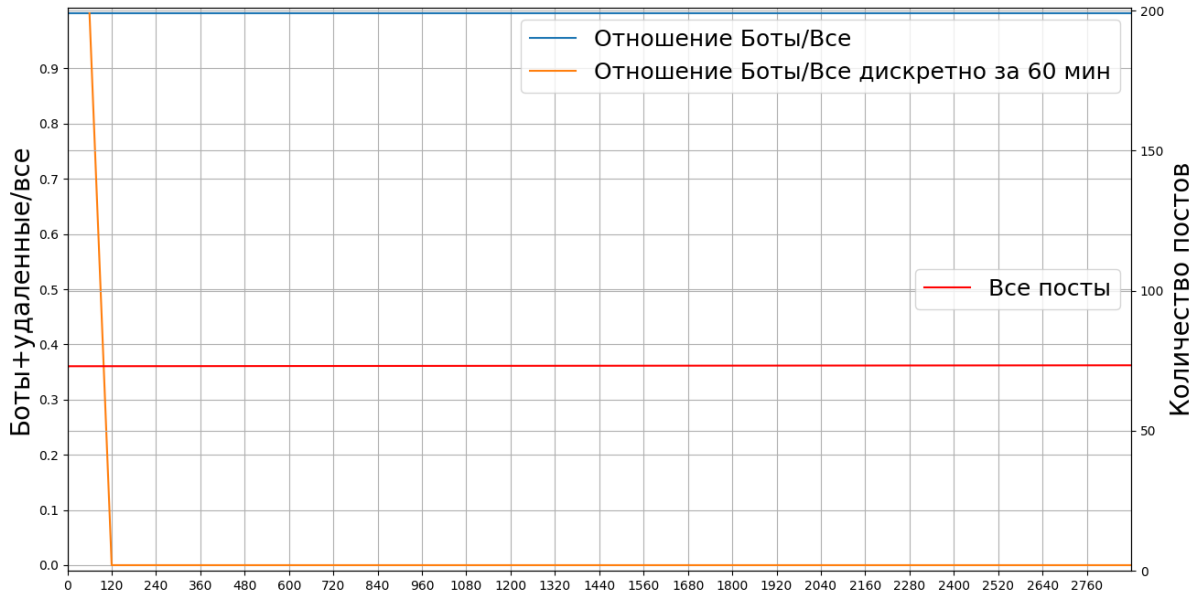

Рис. 4. Практический шаблон 3

Заключение

Проведенные исследования показывают, что злоумышленники активно используют ботов для проведения информационных атак в социальных сетях. Эти автоматизированные программы позволяют им эффективно распространять ложную информацию и манипулировать общественным мнением, что создает серьезные риски для пользователей и общества в целом. Учитывая этот факт, можно сделать вывод, что наблюдение за активностью таких ботов и их поведением в сети может стать важным индикатором для идентификации новых информационных атак.

Список литературы

1. Что такое боты – определение и описание [Электронный ресурс] URL: https://www.kaspersky.ru/resource-center/definitions/what-are-bots (дата обращения: 10.12.2024)
2. Suarez-Lledo V., Alvarez-Galvez J. Assessing the Role of Social Bots During the COVID-19 Pandemic: Infodemic, Disagreement, and Criticism // Journal of Medical Internet Research. 2022. Vol.24. №8. DOI: 10.2196/36085 EDN: IGSQBN
3. Об опасности использования Telegram-ботов [Электронный ресурс] URL: https://www.gazeta.ru/social/news/2023/11/29/21812269.shtml (дата обращения: 10.12.2024)
4. Коломеец М.В., Чечулин А.А. Метрики вредоносных социальных ботов // Труды учебных заведений связи. 2023. Т.9. №1. С.94-104. DOI: 10.31854/1813-324X-2023-9-1-94-104 EDN: HEFHFR
5. Breaking (Bad) Bots: Bot Abuse Analysis and Other Fraud Benchmarks [Электронный ресурс] URL: https://www.arkoselabs.com/wp-content/uploads/Breaking-Bad-Bots-Bot-Abuse-Analysis-and-Other-Fraud-Benchmarks.pdf (дата обращения: 10.12.2024)
6. Aldayel A., Magdy W. Characterizing the role of bots' in polarized stance on social media // Social Network Analysis and Mining. 2022. V.12, №30. DOI: 10.1007/s13278-022-00858-z EDN: TNWDBG
7. Danezis G., Mittal P. SybilInfer: Detecting Sybil Nodes using Social Networks // Conference: Proceedings of the Network and Distributed System Security Symposium, NDSS 2009, San Diego, California, USA.
8. Zhengab X., Zengab Zh., Chenc Zh., Yuab Y., Rong Ch. Detecting spammers on social networks // Neurocomputing. 2015. V.159. P.27-34. DOI: 10.1016/j.neucom.2015.02.047
9. Ботнадзор [Электронный ресурс] URL: https://botnadzor.org/ (дата обращения: 10.12.2024)
10. Программа «Детектор ботов» свидетельство о регистрации программы для ЭВМ регистрационный № 2024617353 от 01.04.2024.
11. API VK для разработчиков [Электронный ресурс] URL: https://dev.vk.com/ru/reference (дата обращения: 10.12.2024)

BOT DETECTION IN SOCIAL NETWORKS

S.V. Bryzgalov, Y.R. Mustakimova, A.N. Rabchevsky
Perm State University

Abstract. The article deals with the problem of using bots in social networks, which are increasingly being used as a means for information attacks. The purpose of this paper is to analyze the current state of methods for detecting and counteracting bots, as well as to develop a program for their detection. With the help of the developed program was analyzed several information attacks conducted in the social network VKontakte. As a result of the research it was concluded that monitoring of bot activity can serve as an important indicator for the identification of new information attacks.
Keywords: *information attacks, social networks, bots, bot detection*.

МОДЕЛЬ АВТОМАТИЗИРОВАННОЙ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ НЕЧЕТКИХ КОГНИТИВНЫХ КАРТ

А.С. Ожгибесова, А.С. Шабуров
Пермский национальный исследовательский политехнический университет

Аннотация. Проанализирована проблема оценки рисков информационной безопасности. Предложено осуществление процесса оценки рисков на основе нечетких когнитивных карт. Приведена последовательность этапов разработки когнитивной модели. Представлен пример разработки нечеткой когнитивной карты на примере объекта критической информационной инфраструктуры.
Ключевые слова: *риск информационной безопасности, защита информации, нечеткая когнитивная карта, объект критической информационной инфраструктуры.*

Оценка рисков информационной безопасности связана с проблемой необходимостью принятия оперативных решений [1]. Данные решения требуют адекватного оценивания параметров и характеристик векторов информационных атак, что также обусловлено разнообразием, сложностью и непредсказуемостью как самих атак, так и прочих деструктивных информационных воздействий. Особенно актуальна данная проблема в условиях внедрения и развития интеллектуальных информационных систем, обеспечивающих функционирование различных, в том числе критически важных процессов и систем [2]. Необходимость оперативного принятия решений по защите информации требует совершенствования процесса оценки рисков, в том числе и за счет автоматизации с использованием компьютерных средств моделирования.

Оценка рисков безопасности информации с использованием нечетких когнитивных карт (НКК) является одним из подходов, который позволяет автоматизировать процесс оценки. Для разработки когнитивной модели, прежде всего, необходимо сформировать множество концептов – значимых факторов с точки зрения оценки рисков информационной безопасности. Следующим шагом является определение силы связи, которая определяет влияние одного концепта на другой и определяется лингвистическими термами. Причем связи между концептами в НКК могут быть как положительными, усиливающими влияние одного концепта на другой, так и отрицательными, которые ослабляют влияние концепта на другой концепт.

Затем составляется НКК с использованием принципов нечеткой логики и теории множеств. Карта представляет собой ориентированный граф, в котором вершинами являются факторы и угрозы безопасности информации, а ребра обозначают влияние этих факторов угрозы [3].

На следующем этапе необходимо задать степень влияния в виде числовых значений или лингвистических термов, таких как «слабое», «среднее» или «сильное» влияние. На основе заданных значений вычисляется уровень опасности угрозы.

По итогу результаты расчета используются для анализа и принятия решений по выбору необходимых мер для усовершенствования системы защиты информации.

В качестве прикладной предметной области для разработки НКК рассматривается одна из транспортных систем, предназначенная для контроля и обеспечения безопасности дорожного движения, реализуемая государственным краевым учреждением «Центр безопасности дорожного движения» (ГКУ ЦБДД).

Поскольку рассматриваемый объект является субъектом критической информационной инфраструктуры (КИИ), оперативная и качественная оценка рисков приобретает особое значение. Непосредственная оценка рисков информационной безопасности рассматривается на примере одного из значимых объектов КИИ – ИС «Метеорологическое обеспечение».

Анализ деструктивных информационных воздействий на ИС «Метеорологическое обеспечение» предполагающий оценку потенциально возможных векторов, которые могут быть реализованы злоумышленником, представлены на рис. 1.

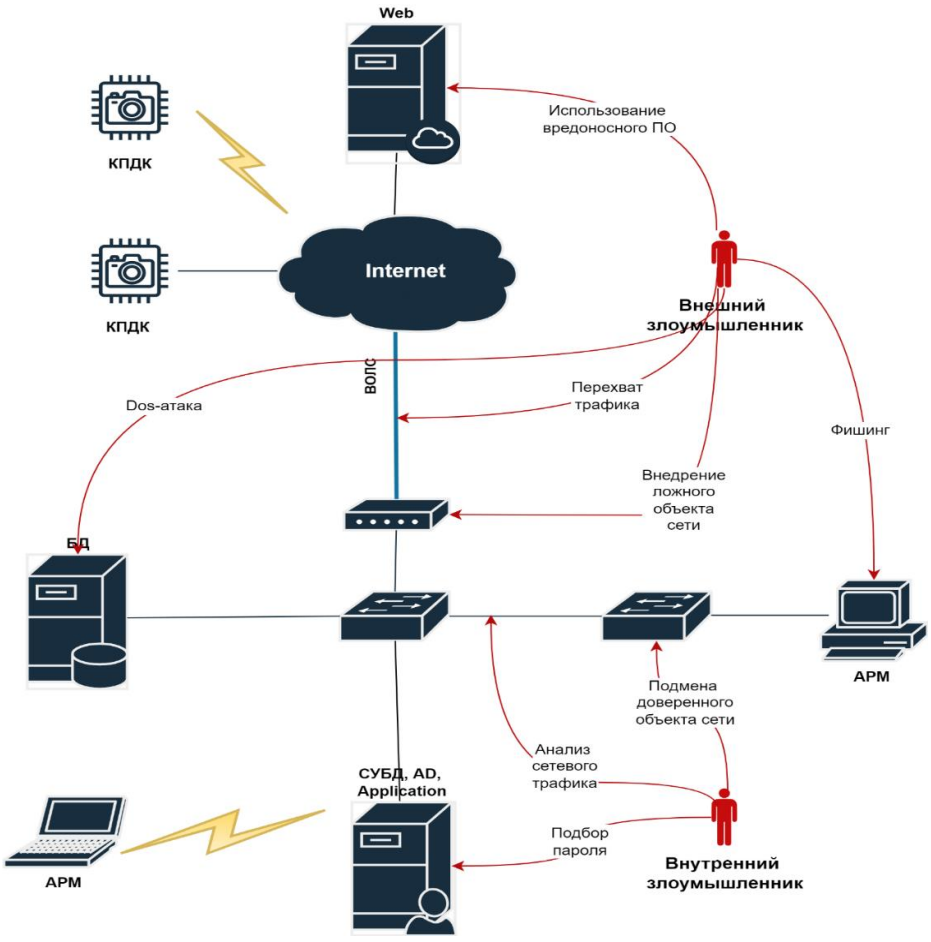

Рис. 1. Вектора атак на ИС «Метеорологическое обеспечение»

Исходя из представленных векторов атак и последствий их реализации, выделяются концепты НКК карты ИС, актуальные для ИС «Метеорологическое обеспечение». Основные концепты когнитивной карты приведены в табл. 1.

Таблица 1

Список концептов НКК

Концепт	Класс	Название концепта	Переменные состояния
C_1	Дестабилизирующие факторы	Угроза анализа сетевого трафика	Среднее количество реализации несанкционированного доступа, в ед. времени
C_2		Угроза сканирования сети	Среднее количество обнаруженных узлов, в ед. времени
C_3		Угроза выявления пароля	Среднее количество подобранных паролей, в ед. времени
C_4		Угроза подмены доверенного объекта сети	Среднее количество подмененных объектов, в ед. времени
C_5		Фишинг	Среднее количество фишинговых атак, в ед. времени
C_6		Угроза внедрения по сети вредоносных программ	Среднее количество вирусных атак, в ед. времени
C_7		Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Среднее количество средств, выведенных из строя, в ед. времени
C_8		Угроза отказа в обслуживании	Среднее количество отказов, в ед. времени
C_9	Информационные ресурсы	АРМ сотрудников	Количество работоспособных АРМ, ед.
C_{10}		КПДК	Количество работоспособных КПДК, ед.
C_{11}		Программное обеспечение	Количество видов ПО, ед.
C_{12}		База данных	Объем информации, содержащейся в БД, Гбайт
C_{13}	Целевые факторы	Репутация организации	Число негативных высказываний, ед.
C_{14}		Качество предоставляемых услуг	Точность метеорологических показаний, %
C_{15}		Материальный ущерб	Финансовые потери, направленные на восстановление работоспособности, руб

В программной среде VUE построена модель оценки рисков НКК (рис. 2), в которой концепты обозначены номерами, а на связях между концептами определены лингвистические значения весов. Значения весов задаются экспертным методом.

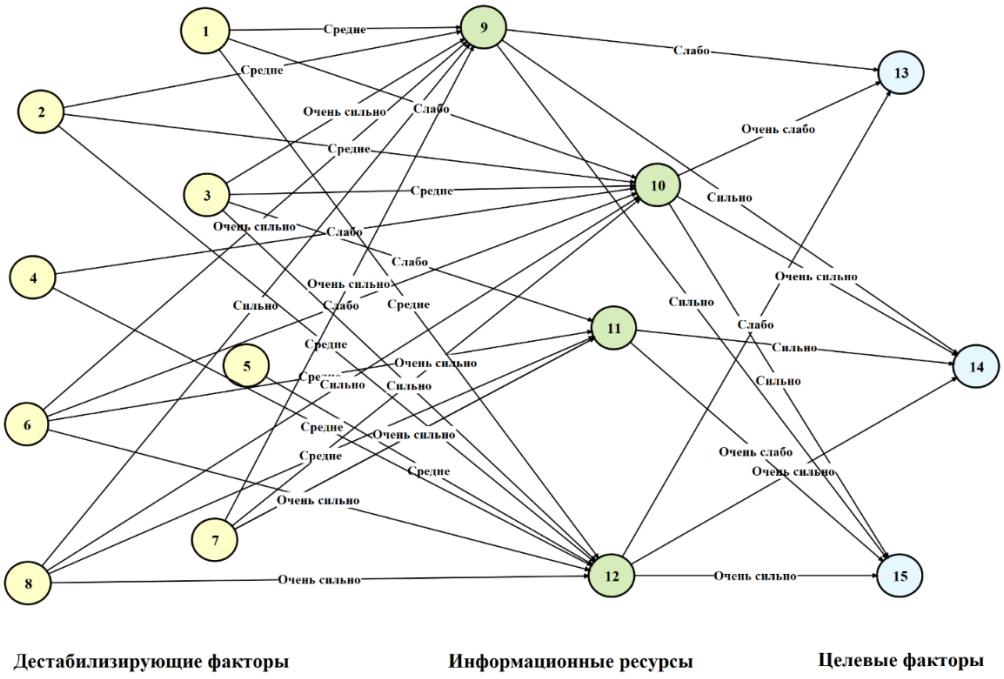

Рис. 2. Модель оценки рисков на основе НКК

Переведенные численные значения лингвистических терм весов связей НКК представлены в табл. 2.

Таблица 2

Веса связей между концептами НКК

Вес связи $C_i \to C_j$	НКК	Вес связи $C_i \to C_j$	НКК	Вес связи $C_i \to C_j$	НКК
W_{ij}	W_{ij}	$W_{4\to12}$	0,475	$W_{8\to12}$	0,925
$W_{1\to9}$	0,475	$W_{5\to12}$	0,475	$W_{9\to13}$	0,250
$W_{1\to10}$	0,250	$W_{6\to9}$	0,925	$W_{9\to14}$	0,725
$W_{1\to12}$	0,475	$W_{6\to10}$	0,250	$W_{9\to15}$	0,725
$W_{2\to9}$	0,475	$W_{6\to11}$	0,475	$W_{10\to13}$	0,100
$W_{2\to10}$	0,475	$W_{6\to12}$	0,925	$W_{10\to14}$	0,925
$W_{2\to12}$	0,475	$W_{7\to9}$	0,925	$W_{10\to15}$	0,725
$W_{3\to9}$	0,925	$W_{7\to10}$	0,925	$W_{11\to14}$	0,925
$W_{3\to10}$	0,925	$W_{7\to11}$	0,925	$W_{11\to15}$	0,100
$W_{3\to11}$	0,250	$W_{8\to9}$	0,725	$W_{12\to13}$	0,250
$W_{3\to12}$	0,725	$W_{8\to10}$	0,725	$W_{12\to14}$	0,925
$W_{4\to10}$	0,250	$W_{8\to11}$	0,475	$W_{12\to15}$	0,925

Расчет состояния i-го концепта НКК производится уравнением вида [5]:

$$X_i(t+1) = f\left(\sum_{j=1}^{n} W_{ji} X_j(t) + X_i(t)\right),$$

где $X_i(t+1)$ и $X_i(t)$ – значения переменной X_i, на $(t+1)$)-м и t-м шаге соответственно, $(k = 1,2,\ldots)$; W_{ji} – вес связи между концептами C_i и C_j; f – некоторая нелинейная функция, принимающая значения в интервале $[0, 1]$.

Расчет относительного уровня риска R_i осуществляется для целевых факторов: (C_{13}), (C_{14}), (C_{15}). Значение уровня угрозы рассчитывается как $R_i = X_i^*$, где X_i^* – установившееся значения состояния -го целевого концепта, в данном случае $i = 13,14,15$. Результаты моделирования уровня угроз целевых факторов показаны в табл.3.

Таблица 3

Результаты моделирования угроз

R_{13}	R_{14}	R_{15}
0,245	0,647	0,925

Таким образом, приведенный в статье пример применения методики оценки рисков безопасности информации для критически важной информационной инфраструктуры ИС «Метеорологическое обеспечение», что оценка рисков, основанная на построении НКК – это эффективный инструмент для анализа нечеткости и неопределенности в оценке угроз безопасности информации и принятия обоснованных решений, что повышает эффективность системы безопасности, в целом. Кроме того, моделирование на основе НКК позволяет учитывать широкий спектр факторов и их взаимосвязей, а также использовать возможность визуализации оценки рисков информационной безопасности. Применение НКК может быть расширено, с учетом новых факторов, характеристик ИС и изменений предметной области. НКК предоставляют собой фундаментальную основу для дальнейшего развития и усовершенствования процесса оценки рисков информационной безопасности.

Список литературы

1. Шабуров А.С. Разработка нечеткой когнитивной модели для автоматизации оценки угроз безопасности информации / А.С. Шабуров, А.С. Ожгибесова // Master’sJournal. – 2023. –№ 2. – Art. № 05. EDN: GVIIEF

2. Ожгибесова А.С., Шабуров А.С. Метод автоматизации оценки угроз безопасности информации на основе нечетких когнитивных моделей // Инновационные технологии: теория, инструменты, практика. – 2022. – Т.1. – С. 290-296. EDN: QQPJBZ

3. Булдакова Т. И., Миков Д. А. Обеспечение согласованности и адекватности оценки факторов риска информационной безопасности // Во-

просы кибербезопасности. 2017. №3 (21). (дата обращения: 04.05.2024). DOI: 10.21581/2311-3456-2017-2-8-15 EDN: YUPXQV

4. Васильев В.И., Вульфин А.М., Герасимова И.Б., Картак В.М. Анализ рисков кибербезопасности с помощью нечетких когнитивных карт. // Вопросы кибербезопасности. 2020. №2 (36). (датаобращения: 21.06.2024). DOI: 10.21681/2311-3456-2020-2-11-21 EDN: BUPCZB

5. Васильев В. И., Вульфин А. М., Кудрявцева Р. Т. Анализ и управление рисками информационной безопасности с использованием технологий когнитивного моделирования // Доклады ТУСУР. 2017. №4. (Датаобращения: 19.05.2024). DOI: 10.21293/1818-0442-2017-20-4-61-66 EDN: YTZQLP

MODEL FOR AUTOMATED INFORMATION SECURITY RISK ASSESSMENT BASED ON FUZZY COGNITIVE MAPS

A.S. Ozhgibesova, A.S. Shaburov
Perm National Research Polytechnic University

Abstract. The article analyzes the problem of assessing information security risks. The implementation of the risk assessment process based on fuzzy cognitive maps is proposed. The sequence of stages of developing a cognitive model is given. An example of the development of a fuzzy cognitive map based on the CII object – IS «Meteorological Support» is presented.

Keywords: *information security risk, information protection, intelligent transport system, fuzzy cognitive map*.

АТАКИ НА КРИТИЧЕСКУЮ ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ КАК ОДИН ИЗ ИНСТРУМЕНТОВ ГИБРИДНОЙ ВОЙНЫ

Ю.А. Паршенкова
МИРЭА – Российский технологический университет

Аннотация. Данная работа посвящена рассмотрению **с**овременных кибератак, которые направлены не только на кражу данных или нарушение работы систем, но и на дестабилизацию целых государств. В условиях гибридной войны, атаки на КИИ могут использоваться для достижения стратегических целей, таких как нарушение работы критически важных объектов, воздействие на экономику и общественное доверие.
Ключевые слова: *кибератака, критическая информационная инфраструктура, гибридная война, угроза безопасности.*

Введение

Критическая информационная инфраструктура (КИИ) является ключевым ресурсом в киберпространстве. Объекты КИИ за последние три года подвергаются постоянным кибератакам. Кража данных, сбои в работе государственных и ведомственных сайтах и многое другое являются примером того, что атаки становятся одним из инструментов в гибридной войне между странами. В связи с этим, для обеспечения национальной безопасности от предприятий и ведомств требуется внедрения современных средств защиты, способных отразить атаки на критически важные объекты.

Примеры регулирования КИИ в мире

В России безопасность КИИ регулируется Федеральным законом от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Этот закон направлен на обеспечение устойчивого функционирования КИИ при проведении компьютерных атак.

Основные положения закона включают:

1. **Определение критической информационной инфраструктуры**: к объектам КИИ относятся информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления, которые играют ключевую роль в различных сферах деятельности.
2. **Категорирование объектов**: объекты КИИ классифицируются по значимости, что позволяет определить уровень их защиты и контроля.
3. **Реестр значимых объектов**: ведется реестр значимых объектов КИИ, что позволяет централизованно управлять их безопасностью.

4. **Оценка безопасности**: проводится оценка состояния защищенности объектов КИИ для выявления уязвимостей и разработки мер по их устранению.

5. **Государственный контроль**: осуществляется государственный контроль за соблюдением требований по обеспечению безопасности значимых объектов КИИ.

6. **Ответственность за нарушения**: предусмотрена ответственность за нарушение требований закона и принятых в соответствии с ним нормативных правовых актов.

Рассмотрим вопрос регламентации КИИ в других странах мира.

К примеру, США в 1986 году первыми закрепили в законе нормы в информационной сфере. В законе прописана ответственность за нарушения, но отсутствует четко сформулированное определение КИИ. Стоит отметить, что при изучении законодательства Штатов и прецедентных норм, можно сделать вывод, что такие преступления фактически приравниваются к посягательству на информационную национальную безопасность [1].

В разных странах Европы также существуют свои подходы к регулированию КИИ.

Так, в Германии особое внимание уделяется защите критической информационной инфраструктуры. Закон «О защите критической информационной инфраструктуры» четко определяет объекты КИИ как информационно-коммуникационные системы и сети, которые играют ключевую роль в различных сферах, таких как энергетика, транспорт и здравоохранение.

Во Франции действует Закон «О защите данных, информационных систем и гражданских свобод», который также определяет критическую информационную инфраструктуру как системы и сети, играющие ключевую роль в обеспечении безопасности, здравоохранения, транспорта и других жизненно важных сфер. Утрата функциональности или уничтожение таких систем может создать серьезные угрозы для национальной безопасности и общественного порядка [2].

В Соединенном Королевстве действует Национальная стратегия кибербезопасности, которая уделяет внимание защите критической национальной инфраструктуры (CNI). Уполномоченные должностные лица компаний, ответственных за обеспечение безопасности, должны идентифицировать критические системы и регулярно оценивать их уязвимость. Органы государственной власти также берут на себя ряд обязательств в этой сфере.

Эти подходы демонстрируют разнообразие и специфику регулирования КИИ в разных странах Европы, подчеркивая важность обеспечения безопасности и защиты критически важных информационных систем.

Если рассматривать вопрос КИИ на примере стран Азии, то в Китае также регламентируются вопросы данной отрасли. Закон «О кибербезопасности КНР» дает четкое определение критической информационной инфраструктуре как общественно-коммуникационной и информационной службе в различных сферах деятельности человека, которая при утрате

функциональности или уничтожении может создать угрозу национальной безопасности.

Мировой опыт показывает, что в большинстве развитых стран за КИИ признают исключительное значение как одной из составляющих безопасности страны. Это подчеркивает важность защиты и устойчивости этих систем для обеспечения национальной безопасности и стабильности.

КИИ как инструмент гибридной войны

КИИ стала мишенью для интенсивных атак в условиях гибридной войны. Злоумышленники с каждым разом улучшают свои вредоносные программы, вирусы, методы перебора паролей, скрипты и другие инструменты. Если вывести из строя хотя бы один элемент КИИ, это может нарушить работу систем автоматизированного управления, что приведет к сбоям и полному прекращению функционирования инфраструктуры.

Наиболее распространенными методами проникновения в корпоративные системы являются взлом периметра и фишинг. Инфостилеры, шифровальщики и вайперы показали высокую эффективность в атаках с использованием ПО. Они применяют кроссплатформенные языки программирования для создания вредоносных программ, что упрощает их компиляцию под различные операционные системы.

Как известно, с введением большого числа санкций и началом СВО, многие иностранные корпорации, являющиеся разработчиками программного обеспечения, приняли решение приостановить выпуск новой продукции, а также поддержку старой, на территории РФ. В связи с этим, Правительством РФ было принято решение о переходе на ПО, разрабатываемое в России. Это не обошло стороной и субъекты КИИ. Данное решение позволило уменьшить влияние иностранных организаций в российском киберпространстве. Основной «всплеск» госзакупок российского ПО пришелся на временной интервал с 2021 по 2022 годы. Для сравнения, до данного периода зарубежное ПО закупалось на сумму около 72 млрд рублей, в то время как на отечественное тратилось порядка 60 млрд рублей в год. В период с 2021 по 2022 годы ситуация резко меняется. Теперь на российское ПО затраты составляют около 103 млрд рублей, а на зарубежное около 53 млрд рублей в год [3].

Внедрение нового отечественного ПО позволит вести борьбу «на своей территории». Собственные методы кодирования и шифрования служат защитой для КИИ, а мониторинг систем программистами помогает выявлять сбои и нарушения. Нестабильная работа КИИ или её полная остановка могут повлиять на национальную безопасность, учитывая, что инфраструктурой владеют не только коммерческие компании, но и государственные учреждения.

Кибератаки как серьёзная угроза безопасности

В период с 2021 по 2023 год мировое киберпространство, включая КИИ, подверглось многочисленным атакам.

По данным исследовательской компании «Cybersecurity Ventures» в 2023 г. киберпреступления происходят по всему миру с интервалом в 10-12 секунд. Стремительный рост кибератак и киберпреступлений прямопро-

порционален увеличению причиняемого ими ущерба во всех отраслях жизни. Так, на сегодняшний день мировой ущерб от киберпреступлений может достигать $6 трлн [3]. При этом 67% кибератак носят целенаправленный характер (рис.).

Рис. Категории жертв среди организаций

Обозначенное носит прогрессирующий характер, что подтверждается аналитическими прогнозами, например, специалистов компании «Positive Technologies», согласно которым в ближайшем будущем рост киберпреступлений будет только расти [3].

Не только сверхдержавы активно борются с киберпреступными группами, но и государства Латинской Америки также страдают от массовых нападений инфостилеров. Например, в апреле 2022 года группа хакеров атаковала ресурсы Министерства финансов Коста-Рики с помощью программы-вымогателя Conti. ИТ-инфраструктура была практически полностью приостановлена, а мошенники потребовали выкуп в размере 20 миллионов долларов у правительства Коста-Рики. В стране было объявлено чрезвычайное положение, а восстановление систем заняло почти месяц.

Значительное количество кибератак в России направлено на государственные учреждения. 10 апреля 2023 года Федеральная таможенная служба (ФТС) России подверглась хакерской атаке, из-за которой была парализована работа Единой автоматизированной информационной системы таможенных органов (ЕАИС ТО). Это привело к простою грузовых машин, который обошелся компаниям в среднем в 5-7 тысяч рублей в сутки.

За период с января по июнь 2024 года количество кибератак увеличилось на 25 %, что указывает на возрастающую роль защиты критической информационной инфраструктуры (КИИ) в обеспечении мировой безопасности. В связи с этим, взаимодействие частного и государственного секторов становится критически важным для создания эффективных и современных механизмов защиты КИИ.

Заключение

Атака на критическую информационную инфраструктуру (КИИ) становится всё более значимым инструментом в гибридной войне. Современные кибератаки направлены не только на кражу данных или нарушение

работы систем, но и на дестабилизацию целых государств. В условиях гибридной войны, атаки на КИИ могут использоваться для достижения стратегических целей, таких как нарушение работы критически важных объектов, воздействие на экономику и общественное доверие. Это требует от государств и организаций разработки и внедрения комплексных мер по защите КИИ, включая усиление кибербезопасности, повышение осведомленности сотрудников и улучшение координации между различными ведомствами. Защита критической информационной инфраструктуры становится не просто вопросом безопасности, а вопросом национальной безопасности и стабильности. Только совместные усилия и комплексный подход могут обеспечить эффективную защиту от современных киберугроз и минимизировать их последствия в условиях гибридной войны.

Список литературы

1. Максимова Е.А. Инфраструктурный деструктивизм субъектов критической информационной инфраструктуры [монография] / Е.А. Максимова// Москва – Волгоград: Волгоградский государственный университет, 2021. – 181 с. – ISBN 978-5-9669-2147-7. – EDN ZZTOKE

2. Максимова Е.А. Оценка информационной безопасности субъекта критической информационной инфраструктуры при деструктивных воздействиях//Монография: Федер. гос. авт. образоват. учреждение высш. образования «Волгогр. гос. ун-т»«.- Волгоград: Изд-во ВолГУ, 2020.- 95 с. ISBN: 978-5-9669-1975-7 EDN: SRVSDQ

3.Актуальные киберугрозы по данным «Positive technologies» [Электронный ресурс]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023/ (дата обращения 01.11.2024).

ATTACKS ON CRITICAL INFORMATION INFRASTRUCTURE AS ONE OF THE TOOLS OF HYBRID WARFARE

Y.A. Parshenkova
MIREA – Russian Technological University

Abstract. This paper is devoted to the consideration of modern cyber-attacks, which are aimed not only at stealing data or disrupting systems, but also at destabilizing entire states. In the context of hybrid warfare, attacks on CII can be used to achieve strategic objectives such as disrupting critical facilities, impacting the economy and public trust.
Keywords: *cyber-attack, critical information infrastructure, hybrid warfare, security threat.*

ИНФОРМАЦИОННОЕ ОРУЖИЕ В КОНЦЕПЦИИ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

А.Н. Рабчевский
Пермский государственный национальный исследовательский университет

Аннотация. Противостояние ведущих мировых держав в современном мире все больше проявляется в виде усиления или обострения информационного противоборства. В статье рассматривается концепция информационного противоборства и обозначается особое место концепции информационного оружия.
Ключевые слова: *информационное оружие, информационное противоборство, методы и способы манипулятивного воздействия.*

Противостояние ведущих мировых держав в современном мире все больше проявляется в виде усиления или обострения информационного противоборства. В связи с этим осознание современного уровня информационного противоборства и применение на практике методов информационного противоборства в целях защиты информационного пространства Российской Федерации является одной из актуальных задач современности.

Однако такое осознание невозможно без принятия современной концепции информационного противоборства. Особое место в этой концепции занимает концепция информационного оружия. В том числе это обусловлено тем, что, не понимая какие виды информационного оружия существуют, невозможно развивать те виды информационного оружия, которых якобы не существует. Это в свою очередь приводит к тому, что государство не развивает такие виды информационного оружия и в результате проигрывает информационную войну. Можно привести аналогию стремительного развития производства БПЛА после того, как боевые действия в зоне СВО показали их необходимость. При этом до начала СВО внимание технологиям БПЛА не уделялось.

Обзор литературы

Если рассмотреть концепции информационного противоборства, существующие в научной среде, то есть несколько основных авторов, которые предпринимали небезуспешные попытки обобщения материала об информационных вонах в виде концепций. Одна из основных работ в этой области, это монография А.В. Манойло [3], в которой представлена концепция информационного противоборства, которая по мнению автора «*представляет* ***совокупность взглядов на цели, задачи, принципы и основные направления*** *информационного противоборства и государственной информационной политики в условиях определения информационным*

обществом новых ***геополитических приоритетов, форм и методов*** *геополитической конкуренции»***.**

Отдельное и очень важное место в концепции выделено информационному оружию, где со ссылкой на зарубежных авторов сказано, что «*Основным инструментом ведения информационных войн является* ***информационное оружие*** *– совокупность средств, методов, способов и технологий информационно-психологического воздействия, специально созданных для тайного управления информационной сферой противника, процессами и системами, функционирующими на основе информации, а также – для нанесения им ущерба. Информационное* ***оружие используется*** *в тайных информационно-психологических операциях* ***в сочетании со средствами*** *и способами его* ***доставки*** *(СМИ, ОТКС, современными средствами связи), технологиями внедрения информационного оружия и технологиями обеспечения условий его использования»*.

Обратим внимание на упоминание средств доставки как отдельной составляющей информационного оружия.

Определение и классификация информационного оружия является одной из задач концепции информационного противоборства. С точки зрения **способа поражения** объектов информационно-психологического противоборства в концепции выделяется **четыре основных типа** информационного оружия:

– средства, методы и способы радиоэлектронной борьбы (РЭБ);

– средства, методы и способы воздействия на программно-техническое обеспечение АИС, ИТКС, АСУ;

– информационные средства, методы и способы воздействия на психику человека с целью модификации его сознания и поведения в нужном для воздействующей стороны направлении;

– средства, методы, способы и технологии дезинформирования системам принятия решений.

В то же время в книге [1] представлена такая классификация информационного оружия:

1. Информационные ***методы и способы скрытного воздействия на сознание человека****: методы воздействия на подсознание человека после введения его в измененное состояние сознания; психокорректирующие компьютерные игры, суггестологические (оказывающие неосознанное внушение) вставки в программные продукты, аудио-, кино- и видеозаписи; методы нейролингвистического и символьного программирования, паранормальные методы (например, экстрасенсорное воздействие вербальными и иными информационными способами).*

2. ***Технологии и способы манипулятивного воздействия на индивидуальное и массовое сознание*** *на психическом, рефлексивном уровне, включающие: внушение (доведение информации, рассчитанное на ее некритическое восприятие, без включения логики и разума), технологии манипулятивного управления, методы рефлексивного управления, принуждение (доведение информации, опирающиеся на наличие чувства страха у человека).*

3. *Второй тип ИО объединяет в себе* ***средства, методы и способы дезинформирования*** *индивидуальных и групповых* ***систем принятия решений*** *с целью выбора ими решений, выгодных дезинформирующей стороне. Основными методами дезинформирования субъектов принятия решений являются навязывание, искажение, блокирование информации, отвлечение на другую информацию.* Основными средствами дезинформирования являются СМИ, средства связи, ТКС.

Если сравнить два этих подхода, то можно увидеть некоторые различия, представленные в табл. 1.

Таблица 1

№	А.Манойло	Л.Воронцова и Д.Фролов
1	Средства РЭБ	–
2	Средства … воздействия на программно-техническое обеспечение АИС, ИТКС, АСУ	–
3	Информационные средства, методы и способы воздействия на психику человека	а. Методы и способы скрытного воздействия на сознание человека. б. Технологии и способы манипулятивного воздействия на индивидуальное и массовое сознание
4	Средства … дезинформирования систем принятия решений	Средства … дезинформирования … систем принятия решений

То есть Л. Воронцова и Д. Фролов, в отличие от А. Манойло, не уделяют внимания техническим аспектам информационного оружия, но более подробно раскрывают психологические методы воздействия на психику человека.

С. Макаренко в своей монографии [2] рассматривает технические и психологические аспекты информационного противоборства. В частности, к средствам и способам информационно-технических воздействий автор относит:

– удаленные сетевые атаки,

– компьютерные вирусы,

– аппаратные и программные закладки,

– нейтрализаторы тестовых программ,

– средства создания ложных объектов информационного пространства,

– средства моделирования боевых действий,

– средства технической и компьютерной разведки, а также

– средства разведки по открытым источникам.

К средствам психологического оружия автор относит:

– лингвистическое,

– психотронное,

– психофизическое,

– сомато-психологическое.

Представлены также основные типы информационно-психологического оружия:

– средства массовой информации,

– средства на основе интернет-ресурсов и социальных сетей,

– когнитивное оружие.

В данном подходе мы видим, что С. Макаренко более подробно раскрывает технические аспекты, детализируя отдельные виды информационно-технических воздействий. Однако, с точки зрения подхода А. Манойло, все эти методы относятся к пункту «*Средства … воздействия на программно-техническое обеспечение АИС, ИТКС, АСУ»*. Показывая различные виды психологического оружия С. Макаренко, детализирует раздел «информационно-психологическое оружие» концепции А. Манойло. Однако помимо психологического воздействия С. Макаренко вводит отдельный вид когнитивного воздействия, чего не было в более ранних работах других исследователей. Таким образом, с учетом представлений С. Макаренко табл. 1 можно было модифицировать следующим образом:

Таблица 2

№	А.Манойло	С.Макаренко
1	Средства РЭБ	–
2	Средства … воздействия на программно-техническое обеспечение АИС, ИТКС, АСУ	– удаленные сетевые атаки, – компьютерные вирусы, – аппаратные и программные закладки, – нейтрализаторы тестовых программ, – средства создания ложных объектов информационного пространства, – средства моделирования боевых действий, – средства технической и компьютерной разведки, а также – средства разведки по открытым источникам.
3	Информационные средства, методы и способы воздействия на психику человека	– лингвистическое, – психотронное, – психофизическое, – сомато-психологическое.
4	Средства … дезинформирования систем принятия решений	
5		– когнитивное оружие.

Развивая свою концепцию информационного противоборства и расширяя данную ранее классификацию, А. Манойло [4] представляет несколько уровней информационно-психологических войны:

– Реализация информационных вбросов – это низовой – тактический уровень ведения ИПВ.

– Следующий – оперативный – уровень предполагает проведение информационных операций, представляющих собой последовательность информационных атак.

– Высший – стратегический – уровень соответствует самой информационно-психологической войне как разновидности международного конфликта.

Эта классификация не предполагает новых типов информационного оружия, но дает возможность оценивать различные виды воздействия с тактической, оперативной и стратегической точек зрения.

В этой статье нам дается четкое определение места информационного противодействия на уровне управления информационными потоками как низовой или тактический уровень информационного противоборства по защите от информационных вбросов. В тоже время ставится задача по разработке системы защиты от информационных вбросов и это должно стать первоочередной задачей научного сообщества.

Сравнивая современные концепции информационных войн в работе [8] показано, что в последнее время информационная война обрела характер ментальной или когнитивной войны, что совпадает с более ранними выводами С. Макаренко [2].

По мнению авторов, концепцию информационного противоборства необходимо воспринимать в комплексной динамике, как это показано на рисунке.

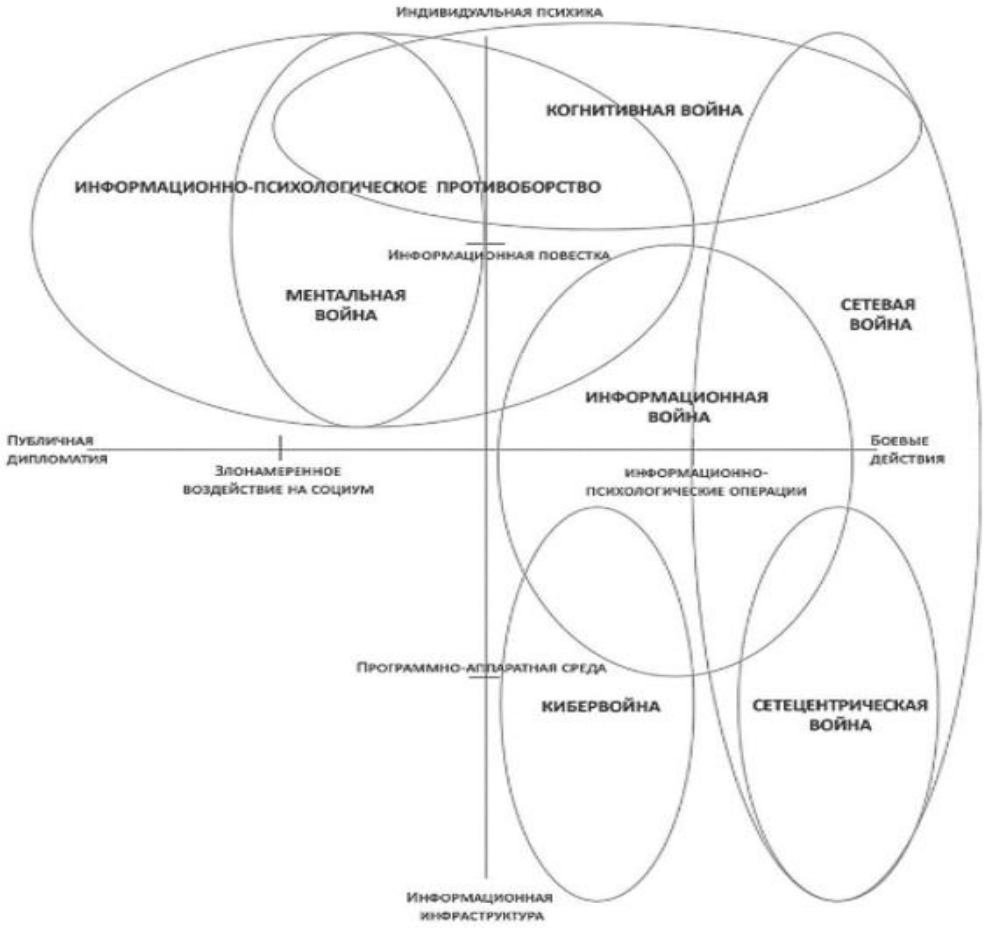

Рис. Сферы информационного противоборства

Как следует из представленной на рисунке схемы авторы выделяют следующие виды противоборства:

– Информационно-психологическое противоборство, в которое входят когнитивная война и информационная война;

– Информационная война, в свою очередь, делится на два раздела, сетецентрическая война и кибервойна.

Такая классификация в общем случае не противоречит концепции А. Манойло, а лишь только некоторым косвенным образом уточняет очевидный факт взаимосвязи различных видов информационного противоборства.

В последующей работе [7] авторы утверждают, что *основной предмет современной концепции информационно-психологического и когнитивного противоборства* включает в себя:

– системы и инструменты формирования общественного мнения, особенности восприятия человеком информации, а также

– весь спектр методов и средств воздействия на общественное мнение и психику отдельного человека в мирное время и в условиях боевых действий с применением специальных информационных и психологических операций стратегического, тактического, оперативного уровня, а также инструментов мягкой силы.

При всех различиях в авторских трактовках и разнице в расстановке исследовательских акцентов *понятие «информационный» (информационное противоборство/война/операция) в первую очередь на первый план выводит воздействие на информационную инфраструктуру, базы данных, каналы коммуникации, программное обеспечение, контроль над информационными потоками и информационной повесткой; понятие «психологический» (психологическая война/операция) фокусирует внимание прежде всего на воздействии на человеческую психику, сознание, эмоции для оказания влияния на поведение человека.*

Из их работы следует, что с одной стороны когнитивное воздействие, как один из видов психологического воздействия, обрело прочное место в общей классификации. С другой стороны, авторы указывают и на технические аспекты воздействия, среди которых указаны *воздействие на информационную инфраструктуру, базы данных, каналы коммуникации и программное обеспечение*, которые можно отнести к противоборству в киберпространстве (см. п. 3 табл. 2). В тоже время, такие методы как *контроль над информационными потоками и информационной повесткой в* явном виде не относятся ни к кибербезопасности, ни к уровню психологического воздействия.

Таким образом напрашивается вывод о том, что необходимо выделить некий отдельный уровень информационного противоборства или информационного оружия, который условно можно назвать **противоборством на уровне информационных потоков**.

Методы

Особое место в информационном противоборстве занимают современные социальные сети, такие как Вконтакте и Телеграм. Деструктивное воздействие в социальных сетях достигается за счет вброса и широкого

распространения деструктивной информации, которая используется в качестве информационного оружия, поражающего подсознание, если производится информационно-психологическое воздействие или на сознание пользователей в случае когнитивного воздействия. Во всех перечисленных выше концепциях предполагается, что если информационное оружие в воздействующей информации задействовано, то есть информация внедрена в социальную сеть, то она непременно достигнет своей цели. Однако, если рассмотреть эту проблему более детально, то выясняется, что это далеко не так. Например, информация может не достигнуть своей цели в случае возникновения препятствий для распространения информации в социальной сети. Технически осуществить это возможно несколькими способами. Так, можно заблокировать наиболее влиятельные узлы, через которые происходят наиболее активные коммуникации. Существуют также и другие технические методы, позволяющие предотвратить распространение информации или по меньшей мере снизить охват пораженной аудитории, снизив тем самым нанесенный ущерб.

Таким образом технические средства, препятствующие распространению деструктивной информации в социальных сетях, можно рассматривать как отдельный вид информационного оружия.

По сути, социальная сеть сама по себе не порождает негативной или позитивной информации, она просто является средой для ее распространения. То есть средством доставки, если пользоваться предложенной выше терминологией. А воздействующая информация, это информационное оружие, которое доставляется до цели, находящейся в этой среде.

Самая простая аналогия, это противовоздушная оборона. Мы же знаем, что, если самолет противника, оснащенный авиабомбами, вылетел для выполнения боевого задания, это не значит, что он точно сможет выполнить свою задачу. Средства ПВО определят, что появилась цель, подлежащая уничтожению, идентифицируют эту цель и затем предпримут попытку уничтожения этой цели.

Точно так же действуют средства противодействия на уровне информационных потоков. То есть, в случае появления деструктивной информации в социальных сетях, специальные методики, описанные в работах [5, 6] могут выявить такую информацию, выявить признаки информационной атаки, а затем предпринять попытки противодействия.

Если вести речь о средствах массовой информации, то там противодействовать информационным технически еще легче.

Выводы

Рассмотрев представленные выше материалы, следую прийти к тому, что существующая концепция информационного оружия должна быть расширена следующим образом:

1. Средства РЭБ;
2. Компьютерная безопасность;
3. Противодействие информационным потокам;
4. Информационно-психологическое воздействие;
5. Когнитивное воздействие.

Принятие такой расширенной версии концепции информационного оружия позволит обратить особое внимание на развитие технических средств информационного противоборства в части технических средств управления информационными потоками и позволит повысить эффективность информационного противоборства. Очевидно, что это может повысить информационную безопасность информационного пространства Российской Федерации.

Список литературы

1. Воронцова Л. В., Фролов Д. Б. История и современность информационного противоборства / Воронцова Л. В., Фролов Д. Б., М.: Горячая линия – Телеком, 2006. 1–192 с.

2. Макаренко С. И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. Монография / Макаренко С. И., Санкт-Петербург: Наукоемкие технологии, 2017. 546 с. ISBN: 978-5-9909412-1-2 EDN: ZFYEUV

3. Манойло А. В. М 23 Государственная информационная политика в особых условиях: Монография. / А. В. Манойло, Москва: М.: МИФИ, 2003. 1–388 с.

4. Манойло А., Пономарева Е. Современные информационно-психологические операции: технологии и методы противодействия // ОБОЗРЕВАТЕЛЬ–OBSERVER. 2019. (2). С. 5–17. EDN: YXSBLN

5. Минаев В. А. [и др.]. Противодействие экстремистской идеологии в социальных медиа: математические модели и методы / В. А. Минаев, К. М. Бондарь, А. Н. Рабчевский, В. Ю. Федорович, Хабаровск: РИО ДВЮИ МВД России, 2023. 1–232 с.

6. Минаев В. А., Рабчевский А. Н., Мустакимова Я. Р. ВЫЯВЛЕНИЕ ИНФОРМАЦИОННЫХ ОПЕРАЦИЙ В СОЦИАЛЬНЫХ СЕТЯХ НА ИХ РАННИХ СТАДИЯХ // ИНФОРМАЦИЯ И БЕЗОПАСНОСТЬ. 2022. № 4 (25). С. 485–494. DOI: 10.36622/VSTU.2022.25.4.002 EDN: HVRAKS

7. Kefeli I. F., Vykhodets R. S. Eurasian Security from the Perspective of the Concept of Information-Psychological and Cognitive Confrontation // EURASIAN INTEGRATION: economics, law, politics. 2023. № 2 (17). С. 11–23. DOI: 10.22394/2073-2929-2023-02-11-23 EDN: DFPBYM

8. Vykhodets R. S., Pantserev K. A. Comparative Analysis of Modern Concepts of Information Warfare // EURASIAN INTEGRATION: economics, law, politics. 2022. № 4. С. 139–148. DOI: 10.22394/2073-2929-2022-04-139-148 EDN: SVTUJU

INFORMATION WEAPONS IN THE CONCEPT OF INFORMATION CONFRONTATION

A.N. Rabchevsky
Perm State University

Abstract. The confrontation of the leading world powers in the modern world is increasingly manifested in the form of strengthening or aggravation of information confrontation. In the article the concept of information confrontation is considered and the special place of the concept of information weapon is marked.
Keywords: *information weapon, information confrontation, methods and ways of manipulative influence.*

ПРОБЛЕМЫ РАЗРАБОТКИ И ПРОИЗВОДСТВА ЭЛЕКТРОННЫХ И МИКРОЭЛЕКТРОННЫХ КОМПОНЕНТОВ В РФ. ПРЕОДОЛЕНИЕ ТЕХНОЛОГИЧЕСКОЙ ЗАВИСИМОСТИ РФ ОТ ВНЕШНИХ ПРОИЗВОДИТЕЛЕЙ

В.А. Родачев, А.В. Черников
Пермский государственный национальный исследовательский университет

Аннотация. В данной работе исследуется вопросы создания и развития собственной радиоэлектронной базы в Российской Федерации. Проводится анализ текущей ситуации: проблемы, возможности, необходимые условия для развития электронных компонентов. Предлагаются возможные решения к формированию независимости Российской Федерации в сфере радиоэлектроники. Описывается проблема отсутствия собственной радиоэлектронной базы с точки зрения информационной безопасности.
Ключевые слова: *импортонезависимость, электронные компоненты, радиоэлектроника.*

В современном мире микроэлектроника используется практически везде, и ни одна страна не может без нее обойтись. К сожалению, в России есть множество проблем с производством электронных компонентов. Из-за отсутствия собственной радиоэлектронной базы проявляются и проблемы Информационной безопасности.

Консалтинговая компания «Яков и партнеры» в отчете «Микроэлектроника России: от дефицита к технологической независимости» (2022 г.) оценила текущую потребность производств в микрочипах базового уровня (90 нм и более) в 30 тыс. пластин в месяц. Сейчас в стране производится только 8 тыс. пластин. Микрочипы менее 45 нм применяются для персональных компьютеров, портативной электроники, серверного оборудования и карт памяти, однако на сегодняшний день спрос на данную номенклатуру чипов со стороны российских производителей остается низким – менее 1 тыс. пластин в месяц. Эти чипы в России не производятся на данный момент. По оценкам компании «Яков и партнеры», в ближайшие пять лет совокупный спрос на чипы в России может вырасти в два раза и достигнуть 60 тыс. пластин в месяц, а в 2030–2035 гг. может превысить отметку в 100–150 тыс. пластин ежемесячно [2]. В связи с отсутствием достаточного предложения на рынке, среди российских производителей микроэлектроники, компаниям приходится закупать компоненты у иностранных изготовителей. Для России одной из важнейших проблем, в использовании иностранных компонентов, является то, что в импортной продукции могут находиться различные закладные устройства, такие как: закладки,

радиомикрофоны, «жучки», «клопы», установленные иностранными разведывательными службами. АНБ устанавливает средства для слежки за трафиком в интернет-роутеры, серверы и другие сетевые компьютерные устройства (оборудование для организации сети связи), которые американские компании поставляют за рубеж, после чего они получают доступ ко всей сети и её пользователям. Об этом стало известно после разоблачения секретных документов Эдвардом Сноуденом. Глен Гринвалд (автор книги «Нигде не спрятаться», написанной на базе разоблачений Сноудена) предполагает, что практика работы АНБ заставила правительство США в 2012 году заподозрить Китайские компании Huawei и ZTE в сотрудничестве со спецслужбами Китая. После проведения расследования и обвинений со стороны США, гендиректор Huawei Рен Женфей в ноябре 2013 г. заявил, что компания уходит с американского рынка [3]. Из вышесказанного, можно сделать вывод, что не только США могут устанавливать «жучки» и заниматься шпионажем, но и другие страны. Поэтому необходимо развивать отечественную микроэлектронику.

Текущее состояние сферы микроэлектроники в Российской Федерации

Большая часть чипов в Россию поступает в виде уже готовых потребительских товаров, таких как ноутбуки, смартфоны, карты памяти и пр. При этом наиболее востребованными с точки зрения промышленности являются микрочипы базового уровня (90 и более нанометров), отсутствие которых может привести к остановке ряда производств. На данный сегмент в 2019 г. приходилось примерно 38% мирового производства (общемировые производственные мощности, выраженные через эквивалент 200-миллиметровых полупроводниковых пластин в месяц).

Ни одно современное производство не может нормально функционировать без микрочипов. Примеры основных сфер применения – информационно-коммуникационные технологии, космическая и авиационная промышленность, а также автомобильная промышленность.

Микрочипы следующего уровня – по нормам 45–90 нм. В целом на сегодняшний день не имеют широкого применения в промышленности, а для современных процессоров и памяти данные нормы являются устаревшими. Всего в мире на них приходится около 9% производства.

Микрочипы продвинутого уровня (менее 45 нм) применяются для персональных и суперкомпьютеров, портативной электроники, серверного оборудования и карт памяти, однако на сегодняшний день спрос на данную номенклатуру чипов со стороны российских производителей остается низким – менее 1 тыс. пластин в месяц.

По оценкам компании «Яков и партнеры», к 2027 году совокупный спрос на чипы в России может вырасти в два раза и достигнуть 60 тыс. пластин в месяц, а в 2030–2035 гг. может превысить отметку в 100–150 тыс. пластин ежемесячно.

При этом в России наблюдается ситуация, в которой, несмотря на явно неудовлетворенный спрос, более 70% мощностей (в собственности компаний НМ-Тех (выкуплены у обанкротившейся «Ангстрем-Т») и Crocus Nano Electronics) не запущено в эксплуатацию. Так, потенциальная производственная мощность оборудования для производства чипов на базовом уровне (>90 нм) в России составляет 26 тыс. пластин в месяц, а фактически используемые мощности позволяют производить всего 8 тыс. Таким образом, запуск производства и настройка его по базовому технологическому процессу могут почти полностью закрыть текущие потребности со стороны промышленности, которые сегодня составляют 30 тыс. пластин ежемесячно, и обеспечить выполнение ключевых задач по формированию устойчивой базы для дальнейшего развития отрасли. Однако с учетом прогнозируемого роста спроса в связи с целями по импортозамещению во многих отраслях необходимо значительное масштабирование производства чипов [2].

Поддержка российской промышленности в области микроэлектроники осуществляется в таких направлениях как:

1. Разработка и построение собственных литографов для производства интегральных компонентов типоразмером 350 нанометров с улучшением этого показателя до 130 нм к 2026 году.

2. Замена оборудования и используемых материалов в процессах изготовления микросхем.

3. Создание большого перечня программно-аппаратных решений для разных этапов и сфер производства микроэлектроники.

4. Предоставление компаниям субсидий в размере 4.2 млрд. рублей на финансирование научных исследований и практику конструирования опытных образцов в 2024 году.

Под освоением 130-нанометровой технологии имеется в виду строительство завода полного цикла производства, на котором будут возможны разработки топологии 90 нм. В последствии размеры транзистора будут уменьшены до условных 65, 45, 28 нанометров и меньше [6].

На сегодняшний день в мире есть всего 2 страны производящие литографическое оборудование для промышленного производства процессоров – Нидерланды и Япония. При этом Японские литографы хороши только для интерконнектов и крупных техпроцессов, т.е. вся современная электроника собирается при помощи машин из Нидерландов.

Как это стало возможным? Только потому, что используются подрядчики из других стран. Технологии подобного уровня требуют компетенций, которые нарабатываются десятилетиями. К примеру, только программное обеспечение под эту машину по объёму кода более чем в 2 раза крупнее, чем ядро операционной системы Linux. Технология изготовления оптических элементов под эти машины разрабатывается годами, и это при высочайшей экспертизе от Zeiss (Немецкая компания, специализирующаяся в области оптики).

В короткий срок произвести это оборудование невозможно. Понадобится 8 лет чтобы научиться делать аналог PAS 5500 (литограф, который закупили для Микрона), учитывая то, что эта машина уже безнадёжно устарела.

К слову, в 2021 году Зеленоградский нанотехнологический центр начал разработку литографического оборудования. Два конкурса Минпромторга на создание установок для печати микросхем на кремниевых пластинах прошли осенью 2021 года: один – на разработку фотолитографа с уровнем топологии до 350 нм, второй – до 130 нм с перспективой его последующей модернизации до топологического уровня 65 нм. В конце 2026 года планируется запуск серийного производства полностью отечественных фотолитографических установок. На проект выделено почти 7 миллиардов рублей [4]. Минпромторг рассчитывает, что в России будет освоено серийное производство микропроцессоров по топологическим нормам 28 нм на 300-миллиметровых кремниевых пластинах в 2027 году.

Более современными технологиями сейчас теоретически может обладать завод «НМ-Тех», запущенный на базе обанкротившегося «Ангстрема-Т». Закупка им оборудования для 28-нм производства была произведена несколько лет назад, но монтаж и наладка еще не завершены.

По данным «дорожной карты» Министерства Торговли и Промышленности, власти рассчитывают, что к 2030 году российские полупроводниковые предприятия сумеют освоить выпуск микроэлектроники по нормам 14 нм.

В Сарове представлена информация о появлении первого «импортозамещенного» демо-литографа в 2025 году. Причем при перспективе освоения с его помощью 28-нм техпроцесса (к 2030-му году) на начальном этапе, то есть к концу 2025 года, обещают представить лишь 90 нм.

На форуме «Микроэлектроника-2023» было объявлено, что в 2024 году на развитие отечественной микроэлектронной промышленности будет выделено госфинансирования на сумму 210 млрд. рублей. Но, для сравнения, около 10 млрд. долларов стоит только одна, причем уже не самая передовая фабрика производства чипов. Также было отмечено, что к 2030 году планируется достичь в данной области импортозамещения на уровне 70% [5].

Научный руководитель Национального центра физики и математики, академик РАН Александр Сергеев сообщил, что «альфа-машина» будет готова в течение двух лет, а версия для предприятий микроэлектроники – еще через три года. Рентгеновский литограф планируют под 28-нм техпроцесс, но на первых порах покажут лишь 90 нм.

Первый демонстрационный образец российского литографа для производства микросхем будет готов в течение ближайших двух лет, а в течение пяти лет ученые планируют изготовить промышленный вариант установки. Об этом ТАСС рассказал научный руководитель Национального центра физики и математики, академик РАН Александр Сергеев.

Основная задача «альфа-машины» – демонстрация того, что все фрагменты технологии работают вместе, а не по отдельности, отметил академик: «Это и источник рентгеновского изучения, и рентгеновская оптика, которая правильным образом проецирует на фоторезисте, это и фоторезисты, и система позиционирования с нанометровой точностью». Причем, уточнил Сергеев, целевое разрешение в 28 нм будет получено не сразу.

«Конечно, это не означает, что через два года там будет разрешение в 28 нанометров. Оно будет улучшаться постепенно. И не за счет того, что мы будем внедрять какие-то новые технологии – технологии мы продемонстрируем сразу, а за счет того, что будет оттачиваться работа. <…> Я думаю, что будет прекрасно, если мы с этими новыми технологиями через два года продемонстрируем 90 нанометров, которые сейчас у нас есть, но уже в слаженной работе всех систем», – сказал он. По словам академика, проект создания литографа финансирует Росатом из своих инвестиционных программ, и этот проект пользуется активной поддержкой правительства страны [7].

В Зеленограде есть строительная площадка, на которой стартовали работы по возведению фабрики. Она, согласно плану, будет выпускать процессоры по 28-нм технологии, которые станут использовать для сборки отечественных электронных устройств разных типов.

Фабрику строят в рамках масштабного плана по развитию отечественной электронной промышленности, одобрен план был еще два года назад, в 2020 году. Национальный проект рассчитан до 2030 года. Автор его – Минпромторг России, в подготовке документа участвовали 22 рабочие группы. Согласно плану, государство планирует вложить в проект 3.19 трлн. руб. Распределять средства будут по четырем основным направлениям – на развитие инфраструктуры, отечественной электронной продукции, повышение спроса на нее и кадровую составляющую.

При этом в плане указано, что до 2024 года планируется обеспечить «100% импортозамещения по всем направлениям», а к 2030 г. «завершить формирование продуктового портфеля российских технологий». На реализацию этого направления выделяется 1.14 трлн. руб. Правда, в другом документе говорится о том, что к 2030 году около 30% российских домохозяйств начнут использовать, в большинстве своем, отечественную электронику. Что касается упомянутых 100%, то эта цифра актуальна для государственных закупок оборудования.

Строительство ведется на месте двух снесенных старых корпусов «Ангстрема». Общая площадь строительства составляет 50 тыс. кв. м. В зданиях будет развернута исследовательская и образовательная инфраструктура Московского института электронной техники. Что касается застройщика, то это Международный научно-технологический центр (МНТЦ) МИЭТ, который создан на базе университета в 2020 году. К слову, для фабрики планировалось закупить 28-нанометровую лабораторно-исследовательскую линию с участком иммерсионной фотолитографии

голландской компании ASML. Но в текущих условиях не совсем понятно, как эта закупка будет выполняться.

При этом планируется обновить всю территорию завода «Ангстрем», вся эта площадка относится к особой экономической зоне «Технополис Москва». Обновление заключается в реконструкции некоторых старых зданий, а также сносе многих ненужных корпусов. Общая площадь зданий, которые находятся на площадке сейчас, составляет около 153 тыс. кв. м. После реконструкции этот показатель увеличится до 500 тыс. кв. м.

Что касается отечественного проекта, то его составители заявляют о разработке к 2030 году не менее 400 прототипов новых видов электроники и о проведении не менее 2000 научно-исследовательских работ.

К 2030 году количество дизайн-центров должно возрасти до 300. При этом в каждом из них планируется создать команду специалистов минимум из 100 человек. Получается, что общее число профильных специалистов составит около 30 000 человек. Но в России достаточно масштабный дефицит IT-профессионалов уже сейчас, и если планируется через 8 лет пригласить на работу 30 тыс. человек, то они, по сути, уже должны поступать в университеты с профильной специальностью.

Вторая проблема, еще более серьезная – оборудование, включая литографические машины. Сейчас говорится о том, что их нужно разрабатывать в России. Но компоненты для таких систем – все сплошь импортные. Возможно, большую часть компонентов можно достать в Китае. Но если хоть чего-то будет не хватать, то производство литографических машин так и не начнется.

Далее – ресурсы для производства чипов. Например, фотошаблоны, производство которых вроде как могут наладить в Зеленограде. Но вот стекла для них нужны импортные, аналогичная ситуация обстоит и с резистом. Кремниевые пластины производят в РФ, но вот слитки, из которых их нарезают – импортные, оборудование для нарезки тоже импортное, равно как и расходные материалы к нему.

Еще одна проблема в том, что завод по производству чипов требует поддержки в сотни миллионов рублей в год, причем неважно, производится на нем что-то или нет. Соответственно, себестоимость продукции может быть очень высокой, если выпускать небольшие объемы чипов. Чем больше объем производства, тем ниже цены. И если у того же Китая внутренний рынок может и будет покупать китайские чипы (процессоры и GPU) миллионами, то в РФ рынок меньше, так что себестоимость чипов в любом случае будет высокой [1].

Возможные пути решения вопроса развития микроэлектроники в стране. Инвестиции в исследования и разработки

Одним из основных способов решения проблемы производства микроэлектроники в России является увеличение инвестиций в исследования и разработки. Это позволит российским компаниям разрабатывать и производить собственные микросхемы. Инвестиции должны быть направлены, в

первую очередь, на развитие передовых технологий, таких как: архитектура, нанометровый техпроцесс и так далее, а во вторую очередь, на развитие крупных производств. Это можно аргументировать тем, что микроэлектроника развивается очень быстро, а на строительство крупных предприятий могут уйти годы, и к тому моменту, когда они начнут работать, выпускаемая продукция уже может стать не актуальна.

Создание инновационных центров и кластеров

Еще одним важным шагом является создание инновационных центров и кластеров, объединяющих исследователей, университеты и предприятия. Эти центры могут служить площадками для совместных проектов, обмена знаниями и трансфера технологий. Они также могут привлекать талантливых молодых специалистов и способствовать их подготовке.

Подготовка квалифицированных кадров

Для развития микроэлектронной промышленности необходимы специалисты в данной области. Российские университеты должны добавить новые и усовершенствовать уже существующие программы обучения (более глубокое изучение литографии, архитектур), чтобы выпускники обладали необходимыми навыками и знаниями. Кроме того, необходимо повышать уровень квалификации действующих специалистов с помощью курсов повышения квалификации и переподготовки.

Сотрудничество с международными партнерами

Россия может сотрудничать с международными партнерами в области микроэлектроники (в данной политической обстановке главным партнером может стать Китай). Это может включать в себя обмен и приобретение технологий, совместную разработку продуктов и создание совместных предприятий. Такое сотрудничество поможет России быстро освоить передовые технологии и получить доступ к глобальному рынку.

Заключение

Решение проблемы производства микроэлектроники в России имеет решающее значение для национальной безопасности и экономического развития. Внедряя описанные выше способы, Россия может преодолеть существующие препятствия, развивать собственную высокотехнологичную промышленность и занять достойное место на мировом рынке микроэлектроники. Этот процесс требует комплексных усилий со стороны правительства, промышленности и образовательных учреждений.

Список литературы

1. [Электронный ресурс] В России начали строить фабрику для выпуска 28-нм чипов. Но все не так просто. URL: https://habr.com/ru/companies/selectel/articles/664260/ (Дата обращения: 15.03.2024).

2. [Электронный ресурс] Яков и Партнёры – Микроэлектроника России: от дефицита к технологической независимости. URL:

https://yakov.partners/publications/microelectronics-in-russia/?ysclid=ltx5kapbjb459853584 (Дата обращения: 15.03.2024).

3. [Электронный ресурс] Агентство национальной безопасности США ставит жучки в экспортное оборудование связи. URL: https://www.comnews.ru/content/82138 (Дата обращения: 15.03.2024).

4. [Электронный ресурс] Будущее российской микроэлектроники / Хабр (habr.com). URL: https://habr.com/ru/articles/661637/ (Дата обращения: 15.03.2024).

5. [Электронный ресурс] «Микроэлектроника-2023»: власти РФ уповают на освоение 28-нм производства чипов к 2027 году. URL: https://russianelectronics.ru/2023-10-11-28-nm-proizvodstva-chipov/?ysclid=lu014cvz2o354538752 (Дата обращения: 15.03.2024).

6. [Электронный ресурс] Микроэлектроника в России 2024: что ждет отрасль в новом году. URL: https://dzen.ru/a/ZZ0O3nVT8X3t9yOY (Дата обращения: 15.03.2024).

7. [Электронный ресурс] Первый российский промышленный литограф может появиться в течение пяти лет – Наука – ТАСС. URL: https://nauka.tass.ru/nauka/18758505?ysclid=lv50bd7dgp998615298&utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru (Дата обращения: 15.03.2024).

PROBLEMS OF DEVELOPMENT AND PRODUCTION OF ELECTRONIC AND MICROELECTRONIC COMPONENTS IN RUSSIA. OVERCOMING RUSSIA'S TECHNOLOGICAL DEPENDENCE ON EXTERNAL MANUFACTURERS

V.A. Rodachev, A.V. Chernikov
Perm State University

Abstract. This paper examines the issues of creation and development of its own radio-electronic base in the Russian Federation. The current situation is analyzed: problems, opportunities, necessary conditions for the development of electronic components. Possible solutions to the formation of independence of the Russian Federation in the field of radioelectronics are offered. The problem of the lack of its own radioelectronic base from the point of view of information security is described.
Keywords: *import-independence, electronic components, radio electronics.*

ЗАДАЧА ПОИСКА ОПТИМАЛЬНОЙ И ЭФФЕКТИВНОЙ ГЛУБИНЫ ПРОВЕДЕНИЯ РЕТРОСПЕКТИВНОГО АНАЛИЗА, В ЦЕЛЯХ ВЫЯВЛЕНИЯ ЗЛОУМЫШЛЕННИКА, НАХОДЯЩЕГОСЯ ВНУТРИ ИТ-ИНФРАСТРУКТУРЫ

М.И. Синцов
Российский государственный университет нефти и газа им. И.М. Губкина

Аннотация. Согласно отчету компании Sophos «The Active Adversary Playbook» в среднем у злоумышленника есть 11 дней после проникновения внутрь ИТ-инфраструктуры, прежде чем они будут выявлены средствами защиты. Первоначальной «точкой входа» хакеров в ИТ-инфраструктуру в сегменте малого и среднего бизнеса является почта (фишинг), уязвимости в ресурсах доступных из вне, либо слабая защищенность конечных точек. В статье рассмотрен вопрос расчёта оптимальной и эффективной глубины проведения ретроспективного поиска, в целях выявления злоумышленника, находящегося внутри ИТ-инфраструктуры.
Ключевые слова: *информационная безопасность, ретроспективный анализ, медианное время пребывания злоумышленника*.

Как долго злоумышленник может оставаться незаметным в ИТ-инфраструктуре предприятия (в разрезе сегмента малого и среднего бизнеса)

Согласно отчету компании Sophos «The Active Adversary Playbook 2021» [1] (фокусируется на продажах решений ИБ в сегменте СМБ) в среднем у злоумышленника есть 11 дней после проникновения внутрь ИТ-инфраструктуры, прежде чем они будут выявлены средствами защиты. Как отмечают исследователи Sophos, этого времени более чем достаточно для получения злоумышленниками полного представления об ИТ-инфраструктуре, ее уязвимостях, подходящих векторах атаки и закреплении. При этом данные из отчета Sophos свидетельствуют о гораздо меньшем времени нахождении злоумышленника, чем данные компании Mandiant (FireEye/Google) [2, 3]. Согласно отчетам Mandiant, среднее время до обнаружения атаки составляло 24 дня в 2020г. (Рисунок 1) и сократилось до 16 дней в 2023 год (Рисунок 2).

Compromise Notifications	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
All	416	243	229	205	146	99	101	78	56	24
External Notification	–	–	–	–	320	107	186	184	141	73
Internal Detection	–	–	–	–	56	80	57.5	50.5	30	12

Рис.1. Медианное время пребывания злоумышленника в ИТ-инфраструктуре (отчет 2021)

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
All	416	243	229	205	146	99	101	78	56	24	21	16
External	–	–	–	–	320	107	186	184	141	73	28	19
Internal	–	–	–	–	56	80	57.5	50.5	30	12	18	13

Рис.2. Медианное время пребывания злоумышленника в ИТ-инфраструктуре (отчет 2023)

Аналитики Sophos объясняют относительно короткое время обнаружения тем, что 81% инцидентов были связаны с действами шифровальщиков, в результате чего парализуется работа организации. Таким образом, с одной стороны, сокращение времени обнаружения может свидетельствовать об улучшении качества работы подразделения ИБ, а с другой – это может быть просто потому, что шифровальщики – максимально заметная и парализующая детальность организации атака, по сравнению, например, с кражей конфиденциальной информации, когда злоумышленник долгое время пытается оставаться незаметным.

Задача поиска оптимальной и эффективной глубины проведения ретроспективного анализа

Ретроспективный анализ ИТ-инфраструктуры – это детальное исследование доступных наборов данных (образов систем, журналов событий ОС, дампов памяти, сетевого трафика, образцов вредоносного ПО, журналов СЗИ и т. д.) за заданный (в большинстве случаев – **максимально доступный, исходя, в частности, из глубины хранения журналов и имеющихся forensic-артефактов**) промежуток времени с целью выявить следы возможной компрометации [4].

Проведем расчет времени в рамках ретроспективного поиска по базе со следующими характеристиками: Размер базы Events – 6000 Гб, среднее количество EPS – 5000, размер базы IoC – 8815 записей.

Введем некоторые ограничения: время поиска не должно превышать более 2 часов, чтобы аналитик в течение рабочего дня мог итерационно провести анализ 3–4 ретроспективных проверок.

Результаты представлены в Таблице № 1.

Соответственно, при глубине поиска более чем 4–6 часов время поиска выходит за изначально выставленные ограничения. При этом, учитывая среднее время нахождения злоумышленника в ИТ-инфраструктуре, нам необходима глубина поиска не менее 11–16 дней.

Таким образом перед нами стоит задача оптимизации времени поиска.

Варианты решения:

1. Уменьшать глубину поиска (объем событий, по которым осуществляется поиск), формировать одновременно несколько задач ретропоиска (10–20 задач, которые перекрывают общую глубину, но небольшими отрезками). Плюсы – за одно и то же время можно покрыть в глубину

большее количество событий. Минусы – большие трудозатраты на аналитика по формированию множества запросов (решается автоматизацией).

2. Уменьшить размер базы IOC по которой осуществляется поиск. Изначально взята общедоступная база IoC FinCERT, которая содержала 8815 IoC IP. При этом дата фиксации в поисковых запросах самой старой записи с IP – октябрь 2023 года. Исходя из среднего времени жизни IoC (Таблица № 2) предлагается исключить индикаторы, которые не встречались в поисках 3 месяца и более. Таким образом получаем 1700 IoC. Что не приводит к сокращению времени поиска, но приводит к сокращению количества выявленных сработок (в т.ч. уникальных). Таблица № 3

3. Оптимизировать запросы поиска.

4. Исключить часть строк, полученных по результатам ретроспективного поиска на основе скоринга IoC/конверсии IoC/других показателях (будут появляться далее по мере выявления зависимости времени поиска от контекста IoC). При этом данное исключение потребует расчёта вероятности того, что в исключенных строчках отсутствуют критичные (с точки зрения выявления злоумышленника) сработки.

Обозначим оптимальную и эффективную глубину проведения ретроспективного поиска – ΔT.

В общем случае ΔT можно представить как зависимость:

$$\Delta T = F\left(N_{IoC}, D_{Depth}, P_{Alert}\right)$$

N_{IoC} – размер базы IoC.

D_{Depth} – глубина ретроспективно поиска (размер базы с событиями).

P_{Alert} – вероятность пропуска критичного события в исключенных строчках.

Кроме того, для нас важными являются еще 2 параметра:

$T_{\text{МВП}}$ – медианное время пребывания злоумышленника в ИТ-инфраструктуре. Для разных сегментов и отраслей среднее время нахождения злоумышленника в ИТ-инфраструктуре различается (Рисунок 1 и 2). За базу предполагается использовать отчеты Mandiant, Sophos, Positive Technologies.

$T_{\text{ВЖ}}$ – время жизни IoC или IoA, которые планируется использовать (Таблица 2). Как правило данное значение указывается поставщиками IoC и IoA. Также можно рассчитывать самостоятельно при ручном поиске IoC и IoA [5, 6]

Значение ΔT будет принадлежать множеству:

$$\Delta T \in (T_{\text{МВП}}; T_{\text{ВЖ}}), \text{при этом если } T_{\text{ВЖ}} \leq T_{\text{МВП}}, \text{то } T_{\text{ВЖ}} = T_{\text{МВП}} + 1 \text{ день}$$

Таблица 1

Среднее время отработки запроса ретроспективного поиска
(Размер базы Events – 6000 Гб, среднее количество EPS в месяц – 5000,
размер базы IoC 8815 записей)

Тип индикатора	**№1**	**№2**	**№3**	**№4**	**№5**	**№6**	**№7**	**№8**	**№9**
Глубина поиска	5 мин	5 мин	15 мин	1 час	2 часа	3 часа	4 часа	6 часов	8 часов
Время поиска	3 сек	2 мин	16 мин	47 мин	67 мин	119 мин	155 мин	200 мин	240 мин
Количество сработок	0	257	1143	4688	10822	106130	132251	160133	210254
Количество уникальных сработок	0	76	214	613	956	1160	1603	1750	1800

Таблица 2

Среднее время жизни типа индикатора.

Тип IoC (IoA)	**IP**	**URL**	**EMAIL**	**DOMAIN**	**SHA / MD**	**TOOLS**	**NETWORK / HOSTS ARTEFACTS**	**TTP**
Время жизни	Дни / Месяцы	Месяцы / Годы	Дни / Месяцы	Месяцы / Годы	Годы	Годы	Годы	-

Таблица 3

Среднее время отработки запроса ретроспективного поиска
(Размер базы Events – 6000 Гб, среднее количество EPS в месяц – 5000,
размер базы IoC 1700 записей)

Тип индикатора	**№1**	**№2**	**№3**	**№4**	**№5**	**№6**	**№7**	**№8**	**№9**
Глубина поиска	5 мин	5 мин	15 мин	1 час	2 часа	3 часа	4 часа	6 часов	8 часов
Время поиска	3 сек	4 мин	11 мин	47 мин	78 мин	120 мин	160 мин	206 мин	237 мин
Количество сработок	0	126	667 \ 684 \ 555	2499	4874	8547	11785	14560	18610
Количество уникальных сработок	0	99	237 \ 241 \ 252	363	411	457	498	509	524

В рамках дальнейших исследований необходимо на практике определить влияние каждого из показателей на увеличение, либо уменьшение ΔT. с использованием различных датасетов При этом в качестве еще одного из условий будет выступать ограниченный набор инструментов, которые могут быть использованы (например в сегменте СМБ как правило нет систем класса Threat Intelligence либо аналогичных)

Список литературы

1. The Active Adversary Playbook – URL: https://news.sophos.com/en-us/2021/05/18/the-active-adversary-playbook-2021/ (дата обращения 10.09.2024).

2. M-Trends 2021 – URL: https://www.mandiant.com/sites/ default/files/2021-09/rpt-mtrends-2021-4.pdf (дата обращения 25.08.2024).

3. M-Trends 2023 – URL: https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2023 (дата обращения 25.08.2024).

4. Итоги расследований инцидентов ИБ в 2021–2023 годах – URL: https://www.ptsecurity.com/ru-ru/research/analytics/outcomes-of-IS-incident-investigations-in-2021-2023-years/ (дата обращения 05.10.2024).

5. Taxonomy driven indicator scoring in MISP threat intelligence platforms – URL: http://arxiv.org/pdf/1902.03914 (дата обращения 10.10.2024).

6. IOCs Are Dead—Long Live IOCs – URL: https://speakerdeck.com/ryankaz/iocs-are-dead-long-live-iocs-rsa-usa-2016 (дата обращения 10.10.2024).

THE PROBLEM OF FINDING THE OPTIMAL AND EFFECTIVE DEPTH OF RETROSPECTIVE ANALYSIS IN ORDER TO IDENTIFY AN INTRUDER INSIDE THE IT INFRASTRUCTURE

M.I. Sintsov
Russian State University of Oil and Gas named after I.M. Gubkin.

Abstract. According to Sophos' report «The Active Adversary Playbook», on average, an attacker has 11 days after penetrating inside the IT infrastructure before they are detected by defenses. The initial «entry point» of hackers into the IT infrastructure in the SMB segment is mail (phishing), vulnerabilities in resources available from the outside, or poorly protected endpoints. The article considers the issue of calculating the optimal and effective depth of retrospective search in order to identify the intruder inside the IT infrastructure.
Keywords: *information security, retrospective analysis, median time of stay of an intruder.*

ИССЛЕДОВАНИЕ СОСТОЯНИЯ БЕЗОПАСНОСТИ ТЕХНОЛОГИИ «ИНТЕРНЕТА-ВЕЩЕЙ»

А.О. Хлопин, А.В. Черников
Пермский государственный национальный исследовательский университет

Аннотация. В статье рассматривается технологии IoT (Интернет вещей) – это сеть, связующая «вещи». Вещь – это устройство, которое выполняет определенную функцию и связанное с другими устройствами посредством сети. Вещь может выполнять как определенную роль, так и совокупность ролей без участия человека. В статье рассматриваются вопросы информационной безопасности технологии IoT.
Ключевые слова: *IoT, безопасность IoT, «умные устройства», проблемы безопасности IoT.*

Интернет вещей – относительно новая технология, которая объединяет множество «умных» устройств в сеть, позволяющую собирать, анализировать, хранить, обрабатывать и передавать друг другу различную информацию. Применение этой технологии на сегодняшний день становится очень обширным. Как пример, в медицине IoT используется для дистанционного мониторинга состояния ЖКТ и обнаружения признаков астмы, в производстве «интернет вещей» помогает в оптимизации производственных цепочек, также IoT используется для контроля сетей связи, водоснабжения и электроснабжении. По данным компании IoT Analytics, число подключений к «интернету вещей» составило 14.8 млрд., а глобальные корпоративные расходы, связанные с IoT, в 2022 году составили приблизительно 201 млрд. долларов. Это на 21.5% больше по сравнению с результатом за предыдущий 2021 год. Очевидно, что эта отрасль стремительно развивается, однако на пути ее развития встречаются трудности, характерные для передовых разработок. На данный момент одной из главных проблем IoT является его уязвимость к кибератакам. С увеличением количества подключенных «умных» устройств, растут риски несанкционированного доступа в IoT-систему.

Таким образом, актуальной задачей является задача защита информации в сфере IoT.

Проблемы информационной безопасности технологии «Интернета вещей»

В настоящее время наблюдается увеличение количества инцидентов (преступлений) в сфере информационной безопасности и информационных технологий. Этому способствует повсеместное распространение сетевых технологий хранения данных и широкое распространение IoT-вещей: в 2018 году число подключенных устройств оценивалось в 22 млрд. с пер-

спективой роста примерно до 40 млрд. к 2025 году по данным исследовательской компании Strategy Analytics. Эти устройства могут содержать уязвимости, которыми могут воспользоваться злоумышленники, и в результате поставить под угрозу конфиденциальность пользователя и общественную безопасность.

Не случайно информационная безопасность IoT вызывает беспокойство у 95 % респондентов опроса, проведенного аналитиками IoT Analytics, причем почти 40 % «очень обеспокоены» возможными уязвимостями Интернета вещей. Таким образом, обеспечение безопасности является одной из основных проблем, связанных с IoT. Причиной этой проблемы является тот факт, что технологии IoT, как и большинство потребительских технологий, разработаны без учета требований информационной безопасности, поскольку основной задачей производителей было минимизировать себестоимость и время разработки, удешевить производство и увеличить объем выпускаемой продукции. В результате подобной политики умные устройства испытывают недостаток в ресурсах. Из-за этого недостатка большинство инструментов безопасности не могут быть установлены в устройствах IoT, что делает устройства легкой «мишенью» для злоумышленников. Хакеры находят уязвимости встроенных систем защиты и могут использовать устройства IoT как инструменты для атак на другие сайты. Злоумышленники, вооруженные технологиями IoT, могут, находясь в виртуальном пространстве, угрожать безопасности и даже жизни людей, и число подобных преступлений растет. Например, Управление по контролю за качеством пищевых продуктов и лекарственных препаратов США (FDA) сообщило, что некоторые кардиостимуляторы (устройство, которое посылает электрические импульсы к сердцу, чтобы установить сердечный ритм и сопутствующие медицинские устройства, уязвимы для взлома. Это означает, что пациенты с кардиостимулятором могут попасть под удар хакеров, которые способны захватить контроль над кардиостимулятором. Цифровые данные IoT являются богатым и часто неисследованным источником информации. Большинство производителей IoT-устройств демонстрируют покупателям функциональность их товара – выполняемые функции и возможности, но не упоминают о технологическом стеке разработки ПО, управляющего этими функциями, и не раскрывают его уязвимостей. Подобные угрозы поднимают важный вопрос: как пользователи умных устройств могут защитить себя? Специалисты по безопасности рекомендуют менять пароли, обновлять приложения и сами устройства, защищать персональные данные [1].

Также проблему незащищённости IoT устройств показывают реальные инциденты. Так, например, в 2016 году была проведена масштабная DDoS – атака. В результате неё пострадали такие компании как: Netflix, Amazon, Twitter. Несколько позже специалисты компании Flashpoint выяснили, что DDoS – атака была организована с использованием IoT-устройств, которые были скомпрометированы злоумышленниками [2]. Также в 2021 году швейцарские хакеры взломали камеры наблюдения

компании Verkada, получив при этом доступ к 150 000 прямых трансляций с камер этой компании. Это были камеры наблюдения внутри зданий государственных организаций, таких как школы, больницы, тюрьмы, и частных компаний [3].

Эти происшествия не могли не вызвать реакции от специалистов в области информационной безопасности, поэтому в 2018 году в Калифорнии был прият закон, направленный на защиту IoT-устройств. Документ обязывает производителей умных устройств генерировать для них уникальные комбинации логина и пароля. Они также могут разработать специальный механизм, который вынудит покупателя изменить стандартные данные для входа при первом запуске.

Проблему безопасности IoT понимают и высокопоставленные лица различных государств. Например, в 2020 году правительство Великобритании обнародовало законопроект, направленный на защиту IoT-устройств [5], а в конце марта 2023 года стало известно о выделении Федеральной службе по техническому и экспортному контролю (ФСТЭК) около 400 млн. рублей на создание отечественного ресурса об уязвимостях автоматизированных систем управления технологическими процессами и промышленного интернета вещей [4].

Также Еврокомиссия прорабатывает «Закон о киберустойчивости» (Cyber Resilience Act) и схему сертификации. По сути, это набор норм, которым должны соответствовать все умные устройства, продаваемые на территории Европейского союза. Правила затронут весь производственный цикл IoT. Разработчики будут сообщать регулятору обо всех обнаруженных уязвимостях, а также предоставлять обновления безопасности на протяжении пяти лет. Стоит заметить, что новые правила не относятся к открытому аппаратному обеспечению (но только если оно не предназначено для продажи). За нарушения предусмотрены оборотные штрафы в стиле GDPR [12].

Также свои услуги в области безопасности IoT оказывают такие компании как Касперский и Майкрософт. Те же компании выпускали статьи о том, как можно защититься от угроз владельцам «умных» устройств [13].

Для борьбы с преступлениями в сфере информационной безопасности был создан специальный раздел криминалистики – компьютерная криминалистика, или форензика – прикладная наука о раскрытии преступлений, связанных с компьютерной информацией, об исследовании доказательств в виде компьютерной информации, методах поиска, получения и закрепления таких доказательств. IoT-криминалистика (англ. IoT-forensics) как подраздел форензики занимается расследованием преступлений в сфере информационной безопасности в системе IoT, исследованием цифровых доказательств.

В ходе расследования компьютерных преступлений, связанных с мошенничествами, или компьютерных атак, средствами которых, так или иначе, являлись сетевые соединения, проводят цифровую экспертизу –

специальное исследование, включающее анализ использования сетевых технологий. В зависимости от места хранения данных в системе IoT эксперты в сфере IoT – криминалистики выделяют три опасных участка в ландшафте киберугроз: облако, сеть и устройство, соответственно выделяются облачная криминалистика, сетевая и криминалистика на уровне устройства IoT [6].

Однако этого недостаточно и необходимо дальше развивать технологии для безопасности IoT.

Возможные пути решения проблем информационной безопасности технологии «Интернета вещей»

Проанализировав инциденты в области безопасности IoT и предпринимаемые меры различных компаний и государств было выяснено, что следующие проблемы являются наиболее актуальными:

1. Большая площадь атаки: угрозы и риски, связанные с IoT, разнообразны и быстро развиваются. Учитывая их влияние на здоровье, безопасность и конфиденциальность пользователей, их опасность нельзя игнорировать. Пользователи могут не знать, что IoT в значительной степени основывается на сборе и обработке больших объемов данных из различных источников, включая и конфиденциальные данные, и обмене ими.

2. Сложность экосистемы: IoT следует рассматривать не как совокупность независимых устройств, а скорее, как богатую, разнообразную и широкую экосистему, включающую устройства, коммуникации, интерфейсы и людей.

3. Отсутствие законодательных актов, норм и стандартов: фрагментированное и медленное принятие стандартов и правил для внедрения мер безопасности и передового опыта в быстроразвивающейся сфере IoT.

4. Широкое применение в критически важных системах: проникновение технологи IoT в критически важные объекты несёт угрозу безопасности целого государства.

5. Сложность внедрения систем безопасности: интеграция систем безопасности – очень сложная задача из-за наличия потенциально противоречивых точек зрения и требований всех заинтересованных сторон. Например, разные устройства и системы IoT могут использовать разные решения аутентификации, при этом их необходимо интегрировать и сделать совместимыми.

6. Экономия производителей: стремительное внедрение IoT и расширенная функциональность умных устройств в нескольких критически важных отраслях предоставляют большие возможности для значительной экономии затрат благодаря использованию таких функций, как потоки данных, расширенный мониторинг, интеграция и многие другие. И наоборот, низкая стоимость, которой обычно отличаются устройства и системы IoT, влечет за собой негативные последствия с точки зрения безопасности. Производители могут ограничивать функции безопасности с целью сниже-

ния затрат, и, следовательно, система безопасности продукта не сможет защитить от определенных типов хакерских атак.

7. Недостаток специалистов: это довольно новая область, и поэтому не хватает людей с подходящим набором навыков и опытом в области безопасности IoT.

8. Отсутствие четко сформулированной ответственности: отсутствие четкого распределения ответственности может привести к двусмысленности и конфликтам в случае инцидента, связанного с безопасностью, особенно с учетом большой и сложной цепочки, характерной для производства IoT-устройств.

9. Отсутствие тестирования и разработки: некоторые производители устройств интернета вещей настолько торопятся вывести на рынок свои продукты, что считают безопасность второстепенным вопросом. В процессе разработки могли быть не учтены угрозы безопасности устройств, а после запуска могут отсутствовать обновления безопасности. Однако степень защиты устройств растет с ростом осведомленности о необходимости обеспечения безопасности интернета вещей [1].

Из-за большого числа проблем в экосистеме Интернета вещей происходят различные инциденты в области безопасности IoT. Выделяют множество угроз, в которые могут негативно сказаться на деятельности компаний, общества или государства. Самыми распространёнными угрозами являются:

1. DDoS – атака при помощи ботнета

Ботнет является предметом исследований с 2000-х годов. Он может нанести значительный ущерб информационной безопасности как отдельных лиц, так и предприятий. Этот тип атаки не направлен непосредственно на сами устройства IoT – они используются для атаки на другие устройства, не обязательно IoT. Сначала вредоносная программа автоматически находит уязвимые устройства IoT, заражает и объединяет их в ботнет, который затем может использоваться для DDoS-атак, перегружая серверы цели вредоносным трафиком [1].

Такая атака может заставить сервис работать с перебоями, например: DDoS – атака была причиной сбоев в работе сервиса «Госуслуги» летом 2022 года [9], или прекратить работу приложения, что понесет за собой материальные потери компании.

2. Атака на датчики, изменение считываемых ими значений или их пороговых значений и настроек

Атакующий манипулирует конфигурацией датчиков, изменяя установленные на них пороговые значения, чтобы разрешить принимать значения, выходящие за пределы допустимого диапазона, что представляет серьезную угрозу для системы и устройств. Поскольку в более крупных устройствах обычно используется множество дублирующих друг друга датчиков, чтобы атака была эффективной, злоумышленнику необходимо

скомпрометировать несколько датчиков: если бы был скомпрометирован только один, показания за пределами диапазона могли бы быть приняты. Показания могут быть скомпрометированы с помощью данных, полученных от остальных датчиков. Воздействие: разрешение датчикам сообщать и принимать неверные значения подвергает риску IoT-среду; неисправный датчик может пропустить скачок напряжения, что приведет к физическому повреждению системы [1].

Например: злоумышленник может манипулировать показаниями прибора, отвечающего за уровень загазованности помещения, что может привести к необратимым последствиям для места, где датчик установлен.

3. Вымогательство с использованием вредоносных программ

Эти атаки осуществляются вредоносным ПО, которое навсегда блокирует доступ к данным жертвы, если не выплачен выкуп. Подобные атаки можно проводить и за пределами IoT-экосистемы, но их можно избежать, обновляя или исправляя прошивку уязвимых устройств. Но в сфере IoT крайне затруднительно производить обновления и закрывать уязвимости, а некоторые IoT устройства нельзя обновить вовсе.

Данная проблема открывает для злоумышленника множество возможных целей для вымогательства. Злоумышленник может взять под контроль умный термостат в середине зимы и потребовать оплату для включения отопления. Он может взять под контроль электросети или системы больниц, требуя выкуп, подвергая риску безопасность людей.

Одним из ярких примеров IoT-шифровальщика является DeadBolt, поразивший тысячи умных устройств компаний QNAP и NAS в 2022 году. Для атаки использовалась уязвимость CVE-2022-27593, позволяющая злоумышленникам модифицировать системные файлы на устройстве. В результате пользовательские файлы оказались зашифрованы, а интерфейс устройства заблокировало сообщение о том, что для восстановления данных нужно заплатить выкуп в размере 0.03 BTC. Производитель выпустил обновление, закрывающее уязвимость, но подобные атаки все еще остаются актуальными [1], [7].

4. Взлом «умного» устройства

Атакующий может произвести взлом устройства, подключенного к сети. Это может заключаться как в манипуляции с конфигурацией или параметрами исполнительных механизмов, заставляющие их использовать неправильные конфигурации, пороговые значения или данные, влияют на их нормальное поведение, сбивают их нормальные рабочие настройки так и возможен полный контроль над устройством.

Например: злоумышленник может заставить некорректно выполнять свои функции автомобиль, или же полностью управлять им. Это может привести к аварии, нарушению логистики и смерти людей в ходе дорожно-транспортного происшествия [10].

Ярким этому примером является взлом автомобиля Tesla в 2020 году. Несмотря на то, что происходил взлом в рамках соревнования, это показы-

вает, что умные автомобили имеют уязвимости. Если взлом будет не в рамках соревнования, то это может повлечь за собой серьезные последствия [11].

Возможные решения проблем по информационной безопасности технологии «Интернета вещей»

В мире безопасности IoT существует множество проблем. Это и сложность самой экосистемы IoT, и недостаток специалистов данной области, и отсутствие точной законодательной базы, и экономия производителей на безопасности. Но стоит выделить 2 основные проблемы, решив которые, можно будет автоматически решить остальные проблемы, если не полностью, то частично.

Первая проблема – это отсутствие законодательных норм и стандартов в области безопасности Интернета – вещей. Необходимо создать стандарты сертифицирования IoT – устройств и создать или назначить компанию, у которой будет право сертифицировать умные устройства. Также можно разделить сертифицирование на типы. Например: 1 уровень будет включать в себя базовые методы обеспечения безопасности, например: шифрование, а последний уровень защиты будет способен противостоять взломам и иметь самую современную защиту. Сам сертификат должен выдаваться на определенный срок, чтобы компании постоянно обновляли защиту умных устройств. В дальнейшем можно внести предложение о создании законопроекта, обязующего производителей сертифицировать свои устройства. Также необходимо постоянно обновлять данный проект и вносить в него поправки в виду новизны и изменчивости экосистемы IoT. В конечном итоге это позволит избавится от части вытекающих проблем. Например: экономия производителей на безопасности. Компаниям будет невыгодно экономить, потому что законопроект будет предусматривать систему санкций по отношению к производителям и им будет невыгодно не устанавливать системы безопасности.

Вторая проблема – это нехватка специалистов. Потребность в специалистах по защите информации растет каждый год [14]. Специалисты в области безопасности IoT не являются исключением. Необходимо увеличивать количество специалистов в сфере IoT безопасности. Для этого необходимо выделять субсидии образовательным учреждениям и ввести курс по IoT – безопасности для переквалификации граждан, так как сейчас специальности в области безопасности Интернета – вещей не существует. В дальнейшем можно предложить создать ответвление от курса информационной безопасности, где студентам рассказывают о безопасности системы IoT или выделить отдельную специальность. Если решить проблему нехватки качественных специалистов, то проблема сложности данной экосистемы будет не столь критичной, так как будут специалисты, которые умеют работать в данной сфере. Также будет решена проблема отсутствия тестирования умных устройств, потому что в компетенции специалистов

должно быть заложено умение тестировать и эксплуатировать решения в области безопасности.

Если решить две данных проблемы, то большая часть проблем будет уже частично решена. Необходимо лишь дополнять программу для специалистов актуальными знаниями, чтобы по завершению обучения получился специалист, знакомый с актуальными предложениями в мире IoT безопасности. А также редактировать законопроект о безопасности Интернета – вещей, чтобы производители знали текущие стандарты и нормы. Чем раньше начать решать проблему, тем больше проблем можно избежать в будущем.

Заключение

В ходе исследования было выяснено, что в экосистеме IoT множество проблем и угроз, которые необходимо решить. Некоторые компании, например, Касперский, уже занимаются решением части проблем, а также создают средства защиты, но этого недостаточно. Поэтому необходимо направить часть инвестиций в эту область, чтобы быть готовым к новым вызовам в будущем.

Список литературы

1. Проблемы безопасности интернета – вещей [электронный ресурс] URL: https://izd-mn.com/PDF/20MNNPU21.pdf (Дата обращения 20.04.2024).
2. DDoS – атака на сервера Dyn [электронный ресурс] URL: https://www.kaspersky.ru/blog/iot-attack/4281/ (Дата обращения 20.04.2024).
3. Взлом камер компании Verkada [электронный ресурс] URL: https://www.gazeta.ru/tech/2021/03/10/13506530/verkada.shtml
4. В ближайшие три года из федерального бюджета ФСТЭК России получит 400 млн. рублей на безопасность промышленного интернета вещей [электронный ресурс] URL: https://cisoclub.ru/v-rossii-vlasti-potratyat-400-mln-rublej-na-bezopasnost-promyshlennogo-iot/ (Дата обращения 20.04.2024).
5. Великобритания готовит закон по защите IoT-устройств [электронный ресурс] URL: https://www.sipnet.ru/news/velikobriteniya-gotovit-zakon-po-zaschite-iot-ustroistv (Дата обращения 20.04.2024).
6. Наука форензика [электронный ресурс] URL: https://ru.wikipedia.org/wiki/Форензика#cite_note-4 (Дата обращения 20.04.2024).
7. Шифровальщик DeadBolt атакует умные устройства компаний NAS, Qnap и Asustor [электронный ресурс] URL: https://habr.com/ru/news/653177/ (Дата обращения 20.04.2024).
8. Обзор угроз для IoT-устройств в 2023 году [электронный ресурс] URL: https://securelist.ru/iot-threat-report-2023/108088 (Дата обращения 20.04.2024).

9. Минцифры сообщило о DDoS-атаках на «Госуслуги» [электронный ресурс] URL: https://www.rbc.ru/technology_and_media/23/06/2022/62b43ea09a7947124625 1381 (Дата обращения 20.04.2024).
10. Чем опасен «интернет вещей»? [электронный ресурс] URL: https://falcongaze.com/ru/pressroom/publications/articles/why-is-iot-so-dangerous.html (Дата обращения 20.04.2024).
11. Хакеры взломали Tesla https://rg.ru/2023/03/29/hakery-vzlomali-tesla-bystree-chem-vladelec-uspel-kupit-kofe.html (Дата обращения 20.04.2024).
12. Защитить IoT-устройства – что предлагают регуляторы https://habr.com/ru/companies/vasexperts/articles/690332/ (Дата обращения 20.04.2024).
13. Проблемы безопасности интернета вещей и передовые методы их решения https://www.kaspersky.ru/resource-center/preemptive-safety/best-practices-for-iot-security (Дата обращения 20.04.2024).
14. Бизнесу не хватает специалистов по кибербезопасности [электронный ресурс] URL: https://iz.ru/1518510/sergei-gurianov/ib-ne-vedaiut-biznesu-ne-khvataet-spetcialistov-po-kiberbezopasnosti (Дата обращения 20.05.2024).

STUDY ON THE SECURITY STATUS OF THE INTERNET OF THINGS TECHNOLOGY

A.O. Hlopin, A.V. Chernikov
Perm State University

Abstract. This article discusses IoT (Internet of Things) technology, which is a network that connects «things». A thing is a device that performs a certain function and is connected to other devices through a network. A thing can fulfill both a certain role and a set of roles without human participation. The article discusses the issues of information security of IoT technology.
Keywords: *IoT, IoT security, smart devices, IoT security challenges.*

БЕЗОПАСНОЕ НАХОЖДЕНИЕ ДЕТЕЙ В ИНТЕРНЕТЕ. ЦИФРОВАЯ ГРАМОТНОСТЬ РЕБЁНКА

А.Р. Шаев, Е.Ю. Никитина
Пермский государственный национальный исследовательский университет

Аннотация. В статье рассматриваются наиболее актуальные проблемы и угрозы, с которыми могут столкнуться дети и подростки при использовании сети интернет. В статье рассматриваются дети и подростки, возраст которых не превышает 17 лет и которые используют устройства, имеющие доступ в интернет.
Ключевые слова:*ребёнок, подросток, интернет, фишинг, кибербуллинг, доксинг, вредоносное программное обеспечение, нежелательный контент, вербовка*.

Введение

На сегодняшний день дети – это полноправные пользователи интернета. Наряду со взрослыми они могут беспрепятственно получить доступ почти к любому интернет-ресурсу [19]. Однако эти ресурсы могут содержать опасный для ребёнка контент.

Обеспечение безопасности детей в интернете и развитее в них информационной грамотности является важной задачей и обязанностью современного общества. Во-первых, восприятие и реакция взрослых и детей на контент в интернете может значительно различаться из-за ряда факторов, включая уровень психологического развития, жизненный опыт, уровень эмоциональной стойкости и способность к критическому анализу увиденного – это позволяет легче манипулировать детьми и способствует нарушениям психики у ребенка. Во-вторых, большинство детей сейчас – будущие специалисты в различных областях в будущем. Приходя на работу человек зачастую не знаком с правилами пользования той или иной техники, имеющей доступ в интернет, а информацию, которую пытаются донести до него специалисты по информационной безопасности этот человек не воспринимает с нужной ответственностью и часто пренебрегает ею. [20].

Наиболее распространённые виды опасностей, которым подвержены дети в интернете

Можно выделить 5 наиболее распространённых угроз, которым подвержены дети в сети интернет: фишинг, доксинг, вредоносные программные обеспечения, пропаганда запрещённых организаций и вербовка в них, кибербуллинг.

Фишинг – это вид интернет-мошенничества, при котором злоумышленник получает доступ к конфиденциальным данным пользователя или заражает его устройство вредоносным программным обеспечением. Это достигается путем массовых рассылок электронных писем или сообщений в социальных сетях и других сервисах. Часто в письме содержится ссылка на сайт, который выглядит точь-в-точь как сайт, которым часто пользуется жертва [10]. После ввода логина и пароля или других данных на этом сайте, эта информация попадает в руки злоумышленника.

Немало в списке жертв фишинговых атак и детей [11]. Зачастую дети слишком уверены в себе в вопросах безопасности в интернете [11]. Ребенок может думать, что сможет не попасться на уловки мошенников, и никто и никогда не будет пытаться получить его личные данные или заразить устройство вирусами. Ещё один фактор, которым пользуются злоумышленники – это любопытство ребенка [11, 1]. Любопытство заставляет детей переходить даже по самым подозрительным и опасным на первый взгляд ссылкам и скачивать небезопасные приложения и файлы. Эта проблема в основном касается детей более младшего возраста, т. к. сущность любопытства связана с проявлением ориентировочно-исследовательского рефлекса и вытекающими из него формами познавательной активности [1].

Доксинг – это вид интернет опасности, при котором злоумышленник находит и раскрывает в сети идентифицирующую информацию о комлибо, такую как имя, паспортные данные, номера телефонов, адреса и другие личные данные. Далее эта информация распространяется по сети без согласия жертвы. Цели злоумышленников бывают различными: преследование жертвы, его семьи и знакомых; запугивание, причинение психологического вреда, вымогательство [12]. Согласно опросу 2022 года более 20% людей стали жертвами доксинга. Из числа подвергшихся доксингу 40% людей получали угрозы смертью [12].

Главными инструментами получения информации о персональных данных и личной жизни детей можно назвать фишинг, добровольное согласие на использование персональных данных и анализ контента в социальных сетях ребенка [11, 12]. Многие сервисы заставляют в обязательном порядке перед их использованием разрешить сбор конфиденциальных данных.

Причиной добровольного согласия на использование персональных данных чаще всего является то, что дети зачастую не имеют представления о том, что такое персональные данные и на сколько они и их конфиденциальность и защищенность важны для человека. Поэтому они не задумываясь разрешают использование своих личных данных сервису, ведь отказаться от сбора данных продуктом означает отказаться от использования этого самого продукта, на что не знающие об опасности дети, конечно, не согласятся.

Проведенный в 2023 году опрос [11] показал, что более половины опрошенных детей (55%) признались, что указывали в социальных сетях личную информацию, например своё имя, дату рождения и местоположе-

ние. Причиной этого можно считать нужду в социальном признании и принадлежности [1, 2]: на основе теории самоопределения (Деци и Райан) и теории привязанности, можно утверждать, что люди естественно стремятся к социальной принадлежности и признанию. Для детей и подростков, которые находятся на этапе формирования своего социального «Я», лайки и комментарии в социальных сетях могут выступать в качестве формы подтверждения их социального статуса, самоценности и принадлежности к определённой социальной группе.

Вредоносное программное обеспечение – это программы, специально разработанные и внедряемые для нанесения ущерба устройствам и компьютерным сетям. Одним из самых эффективных способов заразить персональное устройство жертвы среди злоумышленников является фишинг [10].

Ещё один очень популярный способ распространения вредоносного программного обеспечения среди мошенников – это торрент-трекеры. Торрент – это умный способ быстрой загрузки файлов, в котором участвуют сами пользователи. В последнее время риски, связанные с интеграцией в программное обеспечение вредоносного кода через торрент-трекеры, на практике стали превышать 90% [21]. Можно выделить несколько основных причин, по которым дети пользуются торрент-файлами: система вознаграждения в подростковом возрасте очень активна, что делает их более восприимчивыми к мгновенным удовольствиям [3]; желание принадлежности к группе и стремление к высокому социальному статусу [4]: родители зачастую дают детям и подросткам ежемесячно сумму на карманные расходы такую, которой не хватает на покупку каких-либо цифровых продуктов – приложений, игр, подписок на сервисы и т.д. [22].

Интернет – это относительно нерегулируемое место, где члены различных запрещенных организаций могут создавать и распространять пропаганду.

В UNODC [17] считают, что дети и подростки подвержены вербовке чаще, поскольку воспринимают мир по-другому, чем взрослые. Детская социальная и эмоциональная незрелость делает их идеальной целью для вербовщиков. Вербовщики могут легко манипулировать чувством справедливости, стремлением к приключениям или желанием быть принятыми в социуме, что особенно характерно для детского возраста. Подростковый возраст характеризуется поиском идентичности и принадлежности. Это создает благодатную почву для вербовщиков, предлагающих чувство единства и целостности через участие в определенных группах. Деструктивное поведение в данном контексте может служить средством самовыражения и способом противостоять установленным нормам.

Платформы социальных сетей, включая электронную почту, чаты, социальные сети, форумы, видеозаписи и приложения, являются особенно популярными инструментами вербовки, которые могут также использоваться для достижения конкретных целей. Один из методов, который может быть определен как «подготовка почвы», основан на том, что исполни-

тель узнает об интересах того или иного лица, с тем чтобы использовать индивидуальный подход и внушить доверие. Еще один метод напоминает «адресную рекламу», когда с помощью отслеживания поведения пользователей в сети интернет группа выявляет тех, кто может поддаться ее пропаганде, и адаптирует изложение материала под свою целевую аудиторию.

Попав в такую организацию, ребёнок может испугаться сказать родителям или кому-либо об этом, а сам выйти из этой организации он не сможет по ряду причин, наиболее частой из которых является страх. [25]

Кибербуллинг – это форма травли или запугивания, которая происходит через цифровые устройства, такие как смартфоны, компьютеры, и платформы социальных сетей. Он включает в себя отправку, публикацию или деление вредоносного, неприятного или ложного контента о другом лице, часто анонимно.

По данным Всемирной организации здравоохранения [13], около 30% детей подвергаются травле и унижениям в сети, более 10% детей в возрасте до 11 лет регулярно сталкиваются с явлениями кибербуллинга.

Кибербуллинг является серьезной проблемой, оказывающей значительное влияние на психологическое состояние детей. Наиболее частыми последствиями кибербуллинга [5, 6] являются повышенный уровень тревоги и депрессии, снижение самооценки и уверенности, риски для физического здоровья, такие как головные боли, утомляемость, и проблемы с пищеварением. Несформированное чувство самооценки может сделать детей более склонными к унижению и агрессии со стороны сверстников [7]. На разных этапах развития, особенно в периоды, связанные с формированием идентичности и социальной компетентности, недружественные действия со стороны сверстников могут иметь долгосрочное негативное воздействие на их психологическое благополучие [8]. Факторы, такие как низкая самооценка, отсутствие эмоциональной поддержки и неспособность разрешать конфликты могут усилить подверженность детей кибербуллингу [9].

Влияние родителей на информационную грамотность детей в интернете

Влияние родителей на информационную грамотность детей в интернете имеет ключевое значение для обеспечения безопасности и развития положительных навыков в цифровой среде. Защита от деструктивной информационной среды стоит очень остро.

Роль родителей в развитии этой компетенции у детей встречает ряд проблем и вызовов таких, как ограниченные цифровые навыки родителей, проблема отсутствия регулирования использования медиа со стороны родителей, недостаток времени и внимания к ребенку со стороны родителей, информационная неграмотность самих родителей, разрыв в понимании цифрового мира между родителем и ребенком.

К сожалению, малое количество родителей в действительности обучают или способны обучить своих детей информационной грамотности.

А ведь родитель – это пример для ребенка: по опросам [23] около половины детей хотят быть похожими на своих родителей.

Таким образом, необходимо заниматься только обучением детей информационной грамотности недостаточно – нужно также заниматься и обучением взрослого поколения.

Предлагаемый подход к решению задачи

В настоящее время существует множество курсов по информационной безопасности в интернете, как для родителей, так и для детей. Однако, несмотря на имеющиеся обучающие ресурсы, до сих пор немалое количество детей становятся жертвами интернет-опасностей.

С нашей точки зрения главной причиной этого является незнание многими детьми и родителями существования обучающих ресурсов в области информационной безопасности. Другая не менее важная причина – отсутствие осознания важности и целесообразности обучения в области информационной безопасности. В учебной программе школ предусмотрено обучение детей вопросам информационной безопасности и информационной гигиены, но времени на данное обучение выделено крайне недостаточно [23].

Нельзя не отметить, что существует множество технических решений, позволяющих оградить ребёнка от просмотра нежелательных сайтов или от использования вредных, по мнению родителей, для ребёнка приложений. Однако технические решения не используются повсеместно и являются лишь борьбой со следствиями, а не с причинами цифровой неграмотности детей.

По нашему мнению, наиболее эффективным способом решения проблемы информационной безопасности детей в интернете является прежде всего изменение содержания школьной программы, в частности предмета «Информатика и ИКТ», а также повышение информационной грамотности родителей. С нашей точки зрения, такой путь решения проблемы позволит добиться максимального, на сколько это возможно, охвата вышеупомянутой аудитории если не обучением вопросам информационной безопасности, то хотя бы просвещением.

Предлагается следующая модификация школьной программы для 5-9 классов:

1. Добавить тему «Безопасность в сети Интернет», где подробно рассмотреть виды интернет-угроз таких, как фишинг, доксинг, вредоносное программное обеспечение и способы его доставки на компьютер, методы защиты от данных угроз, а также включить практические занятия по распознаванию фишинговых сайтов и мошеннических писем.

2. В теме «Информационная безопасность» разобрать реальные случаи киберпреступлений против подростков, обсудить их последствия. Можно так же показать видео, в которых сами жертвы интернет-преступлений рассказывают о том, как это произошло и какие последствия данные инциденты за собой повлекли.

3. Добавить тему «Персональные данные и их защита», где объяснить ценность личной информации, как злоумышленники могут ей воспользоваться и на сколько серьёзные последствия это за собой влечёт, а также рассмотреть методы ее защиты.

4. В теме «Коммуникационные технологии» рассмотреть вопросы самопрезентации, создания позитивного имиджа в социальных сетях, рассказать детям о интернет-технологиях, помогающих выражать и показывать свои таланты.

В вопросе повышения цифровой грамотности родителей наиболее правильным, на наш взгляд, решением является пропаганда прохождения специализированных курсов в области информационной безопасности, но, в большей степени – регулярное рассмотрение отдельных вопросов информационной безопасности на родительских собраниях в школах, классных чатах и сообществах школ. Рекомендуемые родителям курсы обязательно должны быть бесплатными. В первую очередь родители должны получить объяснения общих принципов безопасного нахождения в сети, использования специализированных средств контроля активности детей). Положительный эффект будет иметь вариант совместного прохождения специализированных заданий и курсов родителей и детей.

Однако, чтобы модифицировать школьную программу, понадобиться исключить из неё некоторые другие темы. Во избежание уменьшения получаемой детьми информации по другим темам можно вынести данные темы на внеучебные мероприятия, проводя их и с детьми, и с родителями.

Таким образом, обучение безопасному использованию интернета должно в основном объеме закладываться в детях в первую очередь в школах, а не на каких-либо специализированных частных курсах, поскольку грамотный в цифровом плане человек – это важный ресурс современного общества.

Список литературы

1. Рубинштейн Л. С. Бытие и сознание. Человек и мир. Издательство «Питер» 2003. – 508 с.

2. Б. Д. Эльконин. Детская психология: учеб. пособие для студ. высш. учеб. заведений – 4-е изд., стер. – М.: Издательский центр «Академия», 2007. – 384 с.

3. Daniel H. Pink Drive. The Surprising Truth About What Motivates Us: Riverhead Books – 2011. – 288 с.

4. Matthew D. Lieberman. Social: Why Our Brains Are Wired to Connect: Crown – 2013. – 384 с.

5. Conor Mc Guckin, Lucie Corcoran. Bullying and Cyberbullying: Prevalence, Psychological Impacts and Intervention Strategies: Hauppauge – 2016. – 276 с.

6. Michelle Wright. The Psychology of Cyberbullying: Nova – 2024 г. – 292 с.

7. Peter K. Smith. The Psychology of School Bullying: Routledge – 2018. – 136c. DOI: 10.4324/9781315516899

8. Эрик Эриксон. Идентичность: юность и кризис: Прогресс, 1996. – 344 с.

9. Leslie Carrol, Rashmi Shetgiri, Dorothy Espelage. Practical Strategies for Clinical Management of Bullying: springer – 2015. – 55 с.

10. Статья издания «Ведомости» «Фишинговые ресурсы в 2023 году массово переезжали в зону .ru» – 2023 г. [Электронный ресурс]. URL: https://www.vedomosti.ru/technology/articles/2024/02/27/1022304-fishingovie-resursi-v-2023-godu-pereezzhali-v-zonu-ru (дата обращения 22.03.2024).

11. Статья компании «Лаборатория Касперского» «Overconfident and over exposed: Are Children Safe Online?» – 2023 г. [Электронный ресурс]. URL: https://media.kasperskydaily.com/wp-content/uploads/sites/86/2023/02/21115456/Kaspersky-State-of-Children-Online-Report-15-02.pdf (дата обращения 22.03.2024).

12. Статья сайта TechReport.com «The 20 Doxxing Statistics You Can't Afford to Ignore in 2023» – 2023 г. [Электронный ресурс]. URL: https://techreport.com/statistics/doxxing-statistics/ (дата обращения 22.03.2024).

13. Европейский портал информации здравоохранения [Электронный ресурс]. URL: https://gateway.euro.who.int/ru/indicators/hbsc_73-been-bullied-once-or-twice/#id=26558 (дата обращения 15.03.2024).

14. Статья компании «Лаборатория Касперского» «Треть родителей в России волнует проблема детской цифровой зависимости» [Электронный ресурс]. URL: https://www.kaspersky.ru/about/press-releases/2023_tret-roditelej-v-rossii-volnuet-problema-detskoj-cifrovoj-zavisimosti (дата обращения 08.04.2024)

15. Статья компании «Лаборатория Касперского» «Какие существуют типы вредоносных программ?» 2023 г. [Электронный ресурс]. URL: https://www.kaspersky.ru/resource-center/threats/types-of-malware (дата обращения 23.03.2024).

16. Статья издания «Ведомости» «Доля пиратов в российской игровой индустрии достигла 70%»- 2023[Электронный ресурс]. URL: https://www.vedomosti.ru/technology/articles/2023/07/20/986111-dolya-piratov-v-rossiiskoi-igrovoi-industrii (дата обращения 29.03.2024).

17. Исследование Управления Организации Объединенных наций по наркотикам и преступности «Пособие по работе с детьми, завербованными и эксплуатируемыми террористическими и воинствующими экстремистскими группами: Роль системы правосудия» – 2019 г. [Электронный ресурс]. URL: https://www.unodc.org/documents/justice-and-prison-reform/Handbook/Russian.pdf (дата обращения 27.03.2024).

18. Отчёт DIGITAL 2022: THE RUSSIAN FEDERATION. – 2022 г. [Электронный ресурс]. URL: https://datareportal.com/reports/digital-2022-russian-federation (дата обращения 20.03.2024).

19. Результаты опроса компании «Лаборатория Касперского» «Исследование: Взрослые и дети в интернете: аналитический отчет.»- 2022 г. [Электронный ресурс]. URL: https://kids.kaspersky.ru/article/vzroslye_i_deti_v_internete_analiticheskiy_otchet_2022_g (дата обращения 21.03.2024).

20. Результаты исследований компании «Лаборатория Касперского» «Около трети российских компаний считают важным проводить тренинги по повышению цифровой грамотности сотрудников»- 2023 г. [Электронный ресурс]. URL: https://www.kaspersky.ru/about/press-releases/2023_okolo-treti-rossijskih-kompanij-schitayut-vazhnym-provodit-treningi-po-povysheniyu-cifrovoj-gramotnosti-sotrudnikov (дата обращения 21.03.2024).

21. Статья издания «Известия» «Качнул не глядя: скрытые опасности использования торрентов» – 2021 г. [Электронный ресурс]. URL: https://iz.ru/1223241/dmitrii-alekseev/kachnul-ne-gliadia-skrytye-opasnosti-ispolzovaniia-torrentov (дата обращения 28.03.2024).

22. Статья издания «Регнум» «Сколько денег дают родители детям на карманные расходы?» – 2021 г. [Электронный ресурс]. URL: https://regnum.ru/news/3213633 (дата обращения 26.03.2024).

23. Статья Полежаева С.В. «Психолог и родители. Как поднять самооценку подростку» [Электронный ресурс]. URL: https://kcsonpz.ucoz.ru/publ/psikholog_i_roditeli_kak_podnjat_samoocenku_podrostku/1-1-0-87(дата обращения 22.03.2024).

24. Рабочая учебная программа по информатике (в соответствии с ФГОС) МКОУ «КАРАУЛИНСКАЯ ОСНОВНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА ИМЕНИ ГЕРОЯ СОВЕТСКОГО СОЮЗА НИКОНОВА КОНСТАНТИНА ПАВЛОВИЧА». 2019. [Электронный ресурс]. URL: https://karaul-school.astr.eduru.ru/media/2019/10/22/1265929801/inf_7-9.pdf (дата обращения 11.04.2024).

25. Статья 20-й городской поликлиники г. Минск. «СИНИЙ КИТ» – СМЕРТЕЛЬНАЯ ИГРА ИЗ СОЦСЕТЕЙ ДЛЯ ПОДРОСТКОВ. РОДИТЕЛИ, БУДЬТЕ ОСОБЕННО ВНИМАТЕЛЬНЫ! [Электронный ресурс]. URL: https://20gp.by/informatsiya/informatsiya-dlya-patsientov/882-sinij-kit-smertelnaya-igra-iz-sotssetej-dlya-podrostkov-roditeli-budte-osobenno-vnimatelny (дата обращения 8.04.2024).

26. Л. Л. Босова, А. Ю. Босова. Информатика 7–9 классы Методическое пособие. Издательство «Москва Бином. Лаборатория знаний» 2016 – 464 с.

KEEPING CHILDREN SAFE ON THE INTERNET. CHILD'S DIGITAL LITERACY

A.R. Shaev, E.Yu. Nikitina
Perm State University

Abstract. The article discusses the most pressing problems and threats that famous children and adolescents face when using the Internet. This article focuses on children and adolescents under 17 years of age who use devices accessible on the Internet.
Keywords: *growth, teenager, Internet, phishing, cyberbullying, doxxing, competitive software, unwanted content, recruitment.*

ИССЛЕДОВАНИЕ ОБУЧЕНИЯ ПЕРСОНАЛА ЗАЩИТЕ ОТ ФИШИНГА И ОЦЕНКА ИХ УЯЗВИМОСТИ

Э.Е. Шубина, Е.Ю. Никитина
Пермский государственный национальный исследовательский университет

Аннотация. В статье рассматриваются современные подходы к обучению персонала, которые направлены на защиту от фишинга, и проведено исследование их влияния на повышение уровня осведомленности и навыков сотрудников. Также был проведен анализ, в ходе которого была выявлена статистика уязвимости персонала перед атаками фишинга. Полученные результаты позволили выявить сильные и слабые стороны в обучении сотрудников организации и предложить рекомендации по совершенствованию программ обучения и повышению общего уровня кибербезопасности в организации.
Ключевые слова: *фишинг, организации, уязвимость персонала, обучение защите от фишинга, кибербезопасность.*

Введение

Фишинг – это форма мошенничества, которая может быть атакой на любого пользователя с доступом к интернету. Цель фишинговой атаки – обмануть человека, чтобы получить доступ к его личным данным или финансовым ресурсам. Чаще всего атаки происходят через электронную почту, социальные сети или веб-сайты, где злоумышленники маскируются под официальные институты, банки или другие организации. После того, как пользователь попадает в ловушку, личные данные и финансовая информация могут быть скомпрометированы.

Для организаций фишинг представляет серьезную угрозу, поскольку утечка конфиденциальной информации может привести к финансовым убыткам и падению репутации.

Обзор литературы

Специалисты компании Positive Technologies провели анализ фишинговых атак, совершенных в отношении компаний в течение периода с 2022 по 2023 год. По результатам исследования было установлено, что 85% всех фишинговых атак были направлены на получение конфиденциальной информации, в том числе 26% с целью финансовой выгоды. [1]

Большинство сложных многоуровневых фишинговых атак, которых приходится 92%, осуществлялись через электронную почту, в то время как сообщения в мессенджерах добавлялись в 8% случаев, а СМС-сообщения использовались лишь в 3% случаев. [1]

В зависимости от целей злоумышленников можно выделить два основных действия, к которым они пытаются привлечь жертву: получение

корпоративных учетных данных или загрузка на рабочее устройство вредоносного файла. Для этого могут быть отправлены сотрудникам электронные сообщения с вредоносным программным обеспечением или с фальшивыми формами ввода информации.

На вредоносное программное обеспечение приходится около 66% содержания фишинговых писем, 20% – на поддельные формы для ввода данных и только 9% – на сообщения без вредоносной нагрузки. [1]

По информации представителей компании BI.ZONE в конце декабря 2023 года количество недобросовестных веб-сайтов в России увеличилось на 86% за 2023 года по сравнению с 2022 годом [1]. Рост числа веб-сайтов, используемых для мошеннических целей, указывает на то, что фишинг остается широко распространенным методом атаки и требует постоянного внимания и защиты.

Если говорить об оценке степени подверженности сотрудников фишингу, то слова Михаила Сухова, руководителя отдела анализа защищенности компании Angara Security, будут говорить о том, что в 10% случаев сотрудники российских компаний не способны определить социотехническую атаку на инфраструктуру компании и переходят по вредоносным ссылкам в фишинговых письмах. Кроме того, в первом полугодии 2023 года число взломов ИБ-инфраструктуры крупных компаний через подрядчиков выросло на 30%. [6]

Исходя из этих слов можно сделать вывод о необходимости улучшения осведомленности персонала. Важно обеспечить обучение сотрудников по выявлению и предотвращению фишинговых атак. Снижение рисков, связанных с человеческим фактором, является одним из ключевых аспектов в обеспечении безопасности данных.

Сегодня организации сталкиваются с задачами повышения осведомленности о кибербезопасности, обеспечения безопасной удаленной работы сотрудников и защиты конфиденциальных данных. Важно также развивать корпоративную культуру в области кибергигиены и измерять уровень осведомленности сотрудников о киберугрозах. Внимание нужно уделять закрытию «уязвимостей» сотрудников и использовать различные подходы к обучению и инструменты для достижения эффективных результатов.

Также нужно помнить о необходимости определения различий в правах пользователей в компании. Сотрудники, имеющие доступ к важной информации, должны быть лучше подготовлены к защите от фишинговых атак. Получение логина и пароля менеджера не столь критично для безопасности системы, как доступ к учетной записи системного администратора.

Существуют следующие способы повышения грамотности сотрудников в вопросах информационной безопасности как часть комплексных мер, которые помогают сотрудникам понимать, как работает фишинг и чего стоит опасаться [7]:

• *Буклеты, памятки.*

В буклетах можно найти информацию о распознавании подозрительных электронных писем и веб-сайтов, обеспечении безопасности личной информации, и действиях при обнаружении подозрительной активности в сети.

При этом следует учитывать, что буклеты могут не всегда быть достаточно эффективны для изменения поведения сотрудников или повышения уровня кибербезопасности в компании. Некоторые работники могут не воспринимать серьезно информацию из буклетов, посчитав ее незначительной, скучной или малоинтересной.

Также стоит отметить, что некоторые сотрудники могут не осознавать серьезность угрозы фишинга или не считать это важным для своей работы, что снижает их мотивацию для изучения материала из буклетов и применения полученных знаний на практике.

• *Лекции.*

Лекции способствуют тому, чтобы сотрудники становились более бдительными и осторожными при обращении с подозрительными сообщениями или запросами.

Однако имеется ограниченность во времени и информации – как правило, они проводятся для достаточно большого количества слушателей и, соответственно, часто являются обобщенными по своему содержанию, не учитывают специфику конкретной компании и ее уязвимости. Кроме того, слушатели могут забыть полученную информацию или недооценить ее важность, если им не дается практический опыт и обратная связь.

Тем не менее лекции по защите от фишинга могут быть полезными в качестве начального обучения, но дополнительные меры, такие как тренировки, симуляции атак и постоянное обновление знаний, также необходимы для эффективной защиты от фишинга.

• *Тренинги.*

Однако у тренингов по защите от фишинга также есть некоторые минусы. Во-первых, не все сотрудники могут отнестись к таким тренингам серьезно или же просто не уделять им достаточно внимания. Кроме того, обучение может оказаться недостаточно эффективным, если не предусмотрены регулярные повторения и обновления материалов, учитывающих новые методы фишинга.

• *Наставничество.*

Наставничество по защите от фишинга может быть полезным в плане разнообразия методов обучения и постоянной актуализации знаний.

В крупных компаниях наставничество неэффективно из-за недостатка специалистов по кибербезопасности, способных обучать тех, кто еще не обладает соответствующими навыками.

• *Электронные курсы / видеоролики / диалоговые тренажеры.*

Электронные курсы с геймификацией и диалоговыми тренажерами были бы самым эффективным и современным вариантом, если бы не от-

сутствие в них практики и контакта с киберугрозой, которые содействуют формированию устойчивых навыков по противодействию фишингу.

Курсы по информационной безопасности требуют определенного уровня технической подготовки и понимания процесса, связанного с соответствием регламентам и кратким изложением этих правил. В результате ответственность за обучение сотрудников о киберугрозах часто ложится на ИБ- и/или ИТ-службы, у которых в большинстве случаев недостаточно педагогической практики. Также для этих служб необходим соответствующий инструментарий для проведения мероприятий по повышению информированности.

Для развития стабильных навыков противодействия фишингу у каждого сотрудника необходимо постоянно не только обновлять знания, но и проводить практические проверки и тренировки.

Одним из методов являются тестирования фишинговых атак, которые помогают уменьшить уязвимость сотрудников к фишингу, а также оценить усвоенный материал. Те, кто не проходит тест, проходят дополнительные курсы. Обучение должно быть систематическим и цикличным для повышения уровня безопасности компании и уменьшения влияния человеческого фактора. Без регулярной практики навыки затухают. Разработка процессов и методологии самостоятельно представляет серьезные трудности.

Более удобным вариантом является обращение к экспертам, которые следят за современными методами киберпреступников и могут предложить меры по повышению киберграмотности сотрудников, учитывая особенности компании.

Злоумышленники используют максимально реалистичные фишинговые атаки, направленные на определенных сотрудников или отделы. Письма составляются таким образом, чтобы не вызывать подозрений, включая профессиональных.

Предлагаемое решение

Для обучения персонала защите от фишинга можно даже не создавать новый метод для того, чтобы улучшить восприимчивость сотрудников к фишингу, достаточно внести некоторые корректировки или применить новый план использования уже существующих методов.

Можно провести параллель с обычным студентом или даже школьником. Предположим, что студент – это сотрудник какой-либо компании, а новая тема по какому-либо предмету – это тема фишинга. Студент в изучении новой темы вначале изучает теоретический материал, и, в большинстве случаев, он не совсем точно может понимать, что, собственно, из себя представляет эта тема, т.к. на теоретических занятиях относительно новая тема может восприниматься студентом довольно абстрактно. Далее он выполняет практические занятия по этой теме и после неё становятся понятны некоторые нюансы, непонятные до этого, начинает налаживаться взаи-

мосвязь между теорией и практикой. Но это ещё не всё. Да, студент изучил теорию, потом выполнил практические задания и, вроде бы, всё стало понятно, но для того, чтобы материал закрепился «в голове» и «остался в ней» на длительное время, нужно ещё раз повторить теоретическую часть. Только после этого происходит конечное преобразование теории и практики в единое целое, заполнение тех «белых пятен в голове», которые появились ещё при изучении теоретической части.

Вернемся к обычному сотруднику компании. Всё, что сказано про студента, можно спроецировать на персонал и продумать план использования методов по обучению защите от фишинга.

В зависимости от отдела, в котором работают сотрудники, можно составить интерактивные вебинары либо онлайн-тренинги. Это и послужит теоретической частью. Главное, чтобы это был такой метод, где преподаватель рассказывает о фишинговых атаках, подкрепляя примерами, и, чтобы у сотрудников была возможность задавать вопросы и взаимодействовать с преподавателем.

Для практической части можно организовать игру или симуляцию по обучению защите от фишинга. Игра может быть разработана с учетом специфики организации и настроена на эмуляцию реальных угроз и типичных схем фишинга. Это позволит сотрудникам освоить методы обнаружения, анализа и предотвращения фишинг-атак, а также научиться принимать быстрые и правильные решения в ситуациях угроз.

Спустя некоторое время после практической части можно дать задание сотрудникам составить отчёт о впечатлениях после проведения обучения и рассказать, что нового они узнали. Это послужит повторением темы после теоретической и практической частей.

Можно также предусмотреть какую-либо награду тому, кто лучше всех в отделе напишет отчёт после прохождения обучения. Важно внести сюда некоторую корректировку: на тренинге можно поделить всех сотрудников на какие-либо группы (в том числе случайным образом). Каждой группе в конце тренинга можно задать какой-либо вопрос, и, если найдётся человек, который на него ответит, то ему можно добавить некоторое количество баллов к отчёту.

Конечно, сотрудники могут использовать всё, что угодно для написания качественного отчёта: интернет, связи, старые материалы и т.д. Однако главная цель компании – это не получение лучшего отчёта, а улучшение осведомлённости персонала компании о том, как распознать фишинг и обходить его. При этом даже если сотрудники будут искать материал «на стороне», не основываясь на своих знаниях, это всё равно послужит для них хорошим повторением и что-то точно запомнится.

Заключение

Исходя из анализа предложенного плана по обучению персонала защите от фишинга, можно заключить, что модификация существующих методов может эффективно увеличить уровень осведомленности сотрудников о фишинге. Проведение интерактивных вебинаров, онлайн-тренингов, игр и заданий для закрепления теории после практических занятий представляет собой комплексный подход к обучению, способствующий более глубокому усвоению материала и развитию навыков защиты от фишинговых атак.

Следует отметить, что эти методы не только помогут сотрудникам освоить новые способы выявления и предотвращения фишинга, но также способствуют формированию ответственного подхода к обеспечению информационной безопасности в компании. Совместимость практики и повторения способствует более глубокому усвоению материала и закреплению знаний, делая их более устойчивыми.

Следовательно, успешная реализация предложенного плана обучения может повысить осведомленность сотрудников компании о фишинге и снизить вероятность успешной атаки, а также создать культуру безопасности в организации. Правильное и грамотное проведение обучения является важным инструментом обеспечения защиты и целостности информации, что в свою очередь способствует повышению общей безопасности бизнес-процессов компании.

Список литературы

1. Тренды фишинговых атак на организации в 2022–2023 годах [Электронный ресурс] URL: https://www.ptsecurity.com/ru-ru/research/analytics/phishing-attacks-on-organizations-in-2022-2023/ (Дата обращения: 12.04.2024).

2. BI.ZONE: 69% корпоративных электронных писем в 2023 году были нелегитимными [Электронный ресурс] URL: https://securitymedia.org/news/bi-zone-69-korporativnykh-elektronnykh-pisem-v-2023-godu-byli-nelegitimnymi.html (Дата обращения: 12.04.2024).

3. TADVISER: Фишинг в России [Электронный ресурс] URL: https://www.tadviser.ru/index.php/Статья:Фишинг_в_России (Дата обращения: 12.04.2024).

4. CYBER MEDIA. Статья: 80% сотрудников попадаются на фишинг [Электронный ресурс] URL: https://securitymedia.org/news/80sotrudnikovpopadayutsyanafishing.html (Дата обращения: 13.04.2024).

5. Досье. Леонид Чуриков, ведущий аналитик компании »СёрчИнформ» [Электронный ресурс] URL: https://biz360.ru/materials/ne-popadayte-na-kryuchok-kak-nauchit-sotrudnikov-raspoznavat-fishingovye-sayty/ (Дата обращения: 13.04.2024).

6. Angara Security: около 10% сотрудников российских компаний попадаются на фишинг [Электронный ресурс] URL: https://iz.ru/1617143/2023-12-08/okolo-10-sotrudnikov-rossiiskikh-kompanii-popadaiutsia-na-fishing (Дата обращения: 14.04.2024).

7. Александр Соколов Руководитель направления Security Awareness (SA) компании «РТК-Солар»: Как повысить киберграмотность персонала и защитить компанию от фишинговых атак [Электронный ресурс] URL: https://www.anti-malware.ru/practice/methods/How-to-increase-staff-cyber-literacy (Дата обращения: 14.04.2024).

STUDY OF STAFF TRAINING IN PHISHING PROTECTION AND ASSESSMENT OF THEIR VULNERABILITY

E.E. Shubina, E.Yu. Nikitina
Perm State University

Abstract. The article considers modern approaches to personnel training, which are aimed at protection against phishing, and conducted a study of their impact on increasing the level of awareness and skills of employees. An analysis was also conducted, which revealed the statistics of staff vulnerability to phishing attacks. The findings revealed the strengths and weaknesses in the organization's employee training and offered recommendations to improve training programs and increase the overall level of cybersecurity in the organization.
Keywords: *phishing, organizations, personnel vulnerability, phishing protection training, cybersecurity.*

Научное издание

Актуальные проблемы информационной безопасности

Сборник статей

Выпуск 1

Издается в авторской редакции
Компьютерная верстка *Е. Ю. Никитина*

Объем данных 3,64 Мб
Подписано к использованию 11.04.2025

Размещено в открытом доступе
на сайте www.psu.ru
в разделе НАУКА / Электронные публикации
и в электронной мультимедийной библиотеке ELis

Управление издательской деятельности
Пермского государственного
национального исследовательского университета
614068, г. Пермь, ул. Букирева, 15