

### **III. Проблемы обеспечения информационной безопасности**

DOI: 10.25728/iccss.2023.75.11.020

**Феокистов С.В., Ермолаев Е.Д.**

#### **Факторы, влияющие на информационную безопасность Российской Федерации, как основа для сценарного моделирования**

**Аннотация:** Развитие технологий порождает новые угрозы в области информационной безопасности. В данной работе выделены ключевые задачи государства и соответствующие им факторы, влияющие на данную систему. На основе этих факторов составлена таблица взаимосвязей факторов и построена имитационная сценарная модель. Разработки позволят исследователям найти подход к обеспечению информационной безопасности, одной из сфер национальной безопасности Российской Федерации.

**Ключевые слова:** информационная безопасность, технологический прогресс, имитационное моделирование, сценарный анализ, национальная безопасность

В наше время информационная безопасность государства становится ключевой составляющей его суверенитета и стабильности. С развитием технологий и увеличением объема цифровых данных информационная безопасность приобретает все большее значение. Угрозы, связанные с киберпреступностью, кибершпионажем, дезинформацией и кибератаками, представляют серьезные вызовы для государств и их граждан. В этом контексте понимание факторов, влияющих на информационную безопасность, становится критически важным.

Актуальность данной темы подтверждается не только наличием угроз, но и быстрым развитием технологий, что дополнительно усиливает сложность задачи обеспечения информационной безопасности. Социальные сети, интернет-платформы, облачные

вычисления и множество других технологий приносят как пользу, так и уязвимости. Исследование и анализ этих факторов с использованием математических, графовых, сценарных моделей предоставляют средства для более глубокого понимания проблемы и разработки эффективных стратегий защиты информационной безопасности государства.

С геополитической точки зрения кибербезопасность стала объектом международных споров и дипломатических усилий. Стремление государств обеспечивать свою информационную безопасность влияет на международные отношения и требует разработки согласованных подходов к проблеме. В странах НАТО с 2008 года организован «NATO Cooperative Cyber Defence Centre of Excellence», на базе которого с 2010 года проходят ежегодные учения Locked Shields, Crossed Swords, Cyber Coalition, повышающие обороноспособность альянса в области информационной безопасности [1]. В России число киберполигонов к 2024 году планируется довести до 15, а также были проведены первые международные учения в сфере кибербезопасности [2].

Наблюдаемый постоянный рост количества киберпреступлений в Российской Федерации на протяжении последних лет [3] подтверждает необходимость в исследовании факторов, влияющих на информационную безопасность государства в рамках решения задачи сценарного моделирования.

Кроме того, в соответствии с указом Президента РФ №400 от 2 июля 2021 года [4], информационная безопасность является одной из основополагающих составляющих национальной безопасности.

Исходя из этого, в настоящее время перед государством стоит ряд задач, направленных на достижение информационной безопасности. Опираясь на них и учитывая технологичность современного мира, можно выделить ряд основных факторов, влияющих на информационную безопасность [5-7]:

- формирование безопасной среды оборота достоверной информации: количество инцидентов с утечкой частной информации;
- предотвращение внутреннего деструктивного информационно-технического воздействия на российские информационные ресурсы: количество зарегистрированных кибератак из-за рубежа;

- предотвращение внешнего деструктивного информационно-технического воздействия на российские информационные ресурсы: количество зарегистрированных кибератак с территории РФ;
- повышение защищенности и устойчивости функционирования единой сети электросвязи Российской Федерации, российского сегмента сети «Интернет»: количество инцидентов, связанных с нарушением работы этих сетей;
- предотвращение и (или) минимизация ущерба национальной безопасности, связанного с осуществлением иностранными государствами технической разведки: количество выявленных случаев технической разведки;
- обеспечение защиты конституционных прав и свобод человека и гражданина при обработке персональных данных: количество жалоб на нарушение прав при обработке персональных данных;
- укрепление информационной безопасности Вооруженных Сил, других войск, воинских формирований и органов: количество инцидентов, связанных с утечкой военной информации;
- противодействие использованию информационной инфраструктуры Российской Федерации экстремистскими и террористическими организациями: количество заблокированных сайтов и аккаунтов, связанных с экстремизмом и терроризмом;
- совершенствование средств и методов обеспечения информационной безопасности на основе применения передовых технологий: количество внедренных новых технологий в области информационной безопасности;
- обеспечение приоритетного использования в информационной инфраструктуре Российской Федерации российских информационных технологий и оборудования: доля использования российских технологий и оборудования в информационной инфраструктуре;
- укрепление сотрудничества Российской Федерации с иностранными партнерами в области обеспечения информационной безопасности: количество заключенных международных соглашений в этой области;
- доведение до российской и международной общественности достоверной информации о внутренней и внешней политике

Российской Федерации: количество публикаций в российских и международных СМИ;

– развитие взаимодействия органов публичной власти, институтов гражданского общества и организаций при осуществлении деятельности в области обеспечения информационной безопасности Российской Федерации: количество проведенных совместных мероприятий, проектов, инициатив.

На основе материалов [5-7] и экспертных знаний для определенных выше факторов построена таблица (таблица 1), в которой представлена взаимосвязь факторов. Равенство веса дуги одному подразумевает положительное влияние фактора  $i$  на фактор  $j$ . Соответственно, отрицательный вес дуги – отрицательное влияние фактора  $i$  на фактор  $j$ .

С целью обеспечения сценарно-экспертной поддержки принятия управленческих решений, направленных на обеспечение информационной безопасности, на основе составленной таблицы взаимосвязей (таблица 1) построена сценарная имитационная модель, представленная в виде ориентированного графа (рисунок 1). Сплошная линия на графе отражает положительное влияние (соответствует весу 1 в таблице взаимосвязей), пунктирная – отрицательное влияние (соответствует весу -1). Стрелка от фактора  $i$  к фактору  $j$  показывает влияние  $i$  на  $j$ .



	<b>Фактор i</b>	<b>Вес дуги</b>	<b>Фактор j</b>
10	Интернет	1	Жалобы
11	Технологическая Разведка	1	Кибератаки заграничные
12	Технологическая Разведка	1	Интернет
13	Жалобы	1	Освещение СМИ
14	Военная утечка	1	Кибератаки заграничные
15	Блокировки	-1	Кибератаки внутренние
16	Блокировки	-1	Жалобы
17	Внедрение	-1	Утечка частной информации
18	Внедрение	-1	Интернет
19	Отечественное ПО	-1	Кибератаки заграничные
20	Международные соглашения	-1	Технологическая разведка
21	Международные соглашения	-1	Военная утечка
22	Международные соглашения	1	Блокировки
23	Освещение СМИ	-1	Жалобы
24	Взаимодействие	-1	Интернет
25	Взаимодействие	1	Внедрение
26	Взаимодействие	1	Отечественное ПО

Разработанная сценарная имитационная модель может быть использована в дальнейших исследованиях, ориентированных на обеспечение информационной безопасности. Представленные факторы, влияющие на информационную безопасность, помогут не только сделать шаг в развитии моделирования данной области, но и идти в ногу со временем в сфере национальной безопасности Российской Федерации с учетом современных тенденций технологического развития.

Литература:

1. The NATO Cooperative Cyber Defence Centre of Excellence. Exercises. – URL: <https://ccdcoe.org/exercises/> (дата обращения 03.11.2023).

2. На ПМЭФ впервые в России прошли международные киберучения. – URL: <https://www.securitylab.ru/news/532363.php> (дата обращения 03.11.2023).

3. Число киберпреступлений в России. – URL: [https://www.tadviser.ru/index.php/Статья:Число\\_киберпреступлений\\_в\\_России](https://www.tadviser.ru/index.php/Статья:Число_киберпреступлений_в_России) (дата обращения 03.11.2023).

4. Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства РФ. – 05.07.2021. – № 27 (часть II). – Ст. 5351.

5. Шульц В.Л., Кульба В.В., Шелков А.Б., Чернов И.В. Сценарный анализ угроз региональной безопасности в информационной сфере / Проблемы управления безопасностью сложных систем: Труды XXII Международной конференции. Москва, декабрь 2014 г. – Москва: РГГУ, 2014. – С. 22-30.

6. Кульба В.В., Шульц В.Л., Шелков А.Б. Информационное управление. Часть 1: Концептуальные основы // Национальная безопасность/NotaVene. – 2009. – №3. – URL: [https://nbpublish.com/library\\_read\\_article.php?id=56751](https://nbpublish.com/library_read_article.php?id=56751) (дата обращения 03.11.2023).

7. Модели и методы анализа и синтеза сценариев развития социально-экономических систем: в 2-х кн. / Под ред. В.Л. Шульца и В.В. Кульбы. – М.: Наука, 2012. Кн. 1. – 304 с., кн. 2. – 358 с.

---

DOI: 10.25728/iccss.2023.77.82.021

**Чернов И.В., Ермолаев Е.Д., Феоктистов С.В.**

**Выделение базисных режимов динамики факторов, влияющих на информационную безопасность Российской Федерации**

**Аннотация:** В данной работе представлен этап разработки методологии сценарного анализа в области