МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ВСЕРОССИЙСКАЯ ГРУППА ТЕОРИИ ИНФОРМАЦИИ IEEE
АКАДЕМИЯ ИНФОРМАТИЗАЦИИ ОБРАЗОВАНИЯ
ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ООО «ОТКРЫТЫЕ РЕШЕНИЯ»
ОБЩЕСТВО «ЗНАНИЕ» РОССИИ
ПРИВОЛЖСКИЙ ДОМ ЗНАНИЙ

XXII Международная
научно-техническая конференция

ПРОБЛЕМЫ ИНФОРМАТИКИ В ОБРАЗОВАНИИ, УПРАВЛЕНИИ, ЭКОНОМИКЕ И ТЕХНИКЕ

Сборник статей

Декабрь 2022 г.

Пенза

УДК 004
ББК 32.81я43+74.263.2+65.050.2я43
П781

П781 **ПРОБЛЕМЫ ИНФОРМАТИКИ В ОБРАЗОВАНИИ, УПРАВЛЕНИИ, ЭКОНОМИКЕ И ТЕХНИКЕ :**
сборник статей XXII Международной научно-технической конференции. – Пенза: Приволжский Дом знаний, 2022. – 356 с.

ISBN 978-5-8356-1800-2
ISSN 2311-0406

Под редакцией ***В.И. Горбаченко,*** доктора технических наук, профессора;
В.В. Дрождина, кандидата технических наук, профессора

Информация об опубликованных статьях предоставлена в систему Российского индекса научного цитирования (РИНЦ) по договору № 573-03/2014К от 18.03.2014.

ISBN 978-5-8356-1800-2
ISSN 2311-0406

XXII International
scientific and technical conference

PROBLEMS OF INFORMATICS IN EDUCATION, MANAGEMENT, ECONOMICS AND TECHNICS

December, 2022

Penza

УДК 004

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ – ПРОБЛЕМЫ ПЕРЕДАЧИ И ЗАЩИТЫ ИНФОРМАЦИИ. ИНФОРМАЦИОННЫЕ ВОЙНЫ

А. Ю. Абашкина, С. С. Яковлева

INFORMATION TECHNOLOGIES - PROBLEMS OF INFORMATION TRANSFER AND PROTECTION. INFO WARS

A. Yu. Abashkina, S. S. Yakovleva

Аннотация. Проанализирована проблема современного ведения пропаганды в информационном обществе. Рассмотрена проблема информационных войн и их влияние на изменения сознания человека.

Ключевые слова: информационная война, информационное общество, психологические операции, электронные ресурсы.

Abstract. The problem of modern propaganda in the information society is analyzed. The problem of information wars and their impact on changes in human consciousness is considered.

Key words: information warfare, information society, psychological operations, electronic resources.

В настоящее время человек живет в информационном обществе. Для общения, работы и существования в обществе люди используют информацию и знания. В настоящее время информационный поток достигает высокого уровня во всех сферах жизни, например в таких, как экономическая и социальная. Любой конфликт или недопонимание между людьми, определенными классами общества, взаимоотношение государств являются в первую очередь информационными. Люди используют информационные ресурсы в различных целях, в том числе для принятия решений, оценки ситуации и формирования собственного мнения.

Следует рассматривать информационную войну как целенаправленное внедрение дезинформации, с целью получения тактического и психологического преимущество над оппонентом.

Именно в связи с высоким потоком информатизации и развитием информационных ресурсов такое понятие, как «Информационная война» набирает обороты и широко используется в современном мире. Смело можно сказать, что именно во время «машинной» эры зародилась главная роль инструмента информационной атаки.

Информационная война, достаточно сложное по своей структуре понятие и явление (рисунок 1).

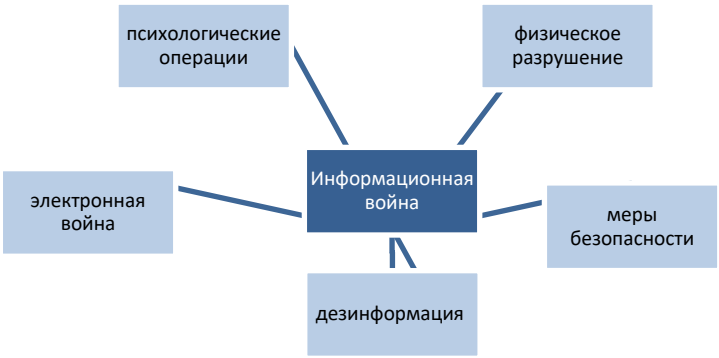

Рис. 1. Составные части информационной войны

Психологические операции – пропаганда, направленная на лиц, не задействованных напрямую в конфликте. Они в основном направлены именно на враждебные, дружественные и нейтральные аудитории, чтобы повлиять на их отношения и поведение, что напрямую является психологическим воздействием.

Электронная война – внедрение через электронные ресурсы. Атака, поступившая таким образом, не дает возможности объекту, против которого она направлена, подтвердить или опровергнуть подлинность информации.

Дезинформация – внедрение и предоставление заведомо ложной информации лицу или группе лиц. Дезинформация направлена на изменение сознания человека и его отношения к той или иной ситуации, трактуя информацию определенным образом.

Физическое разрушение – может также относиться к информационной войне, если говорить о воздействии на информационные системы. Информационные войны вполне могут в ближайшее время вытеснить методы современного ведения пропаганды и стать их главным оружием.

В информационных войнах не применяется прямое насилие, их цель - тактическое и психологическое преимущество перед объектом. Это показывает, что данный вид войн является лишь посредственным средством противостояния, а не его конечной целью. Используя информационные войны, можно достичь превосходства над противником в различных

сферах, не только в социальной и политической, но также и в научно-технической, военной, духовной и экономической. Информационная война способна привести к неблагоприятным последствиям. Как и любая война, она имеет характер нанесения вреда и ущерба. Из-за интенсивного развития в информационной сфере, информационная война способна вызвать религиозные, национальные и даже мировые информационные катастрофы. Последствия таких катастроф могут быть губительными для всего человечества. Поэтому вместе с развитием технологии информационных войн, развиваются и меры безопасности от их воздействия.

Основные меры безопасности - предупреждение и блокирование возможных утечек секретной информации, предотвращение намерений информационных атак. Источники угроз информационной безопасности государств делятся на внешние и внутренние.

К внешним источникам можно отнести:

отрыв от развития конкурентоспособных информационных технологий ведущих держав мира;

разработка концепций информационных войн другими странами, которые могут повлечь за собой нарушения сохранности информационных ресурсов страны или несанкционированный доступ к ним;

вытеснение с внешнего и внутреннего информационных рынков, в последствии доминирования ряда стран в мировом информационном пространстве;

любая деятельность, направленная против информационной сферы, какого-либо государств, например политической, военной.

К внутренним в свою очередь относятся:

недостаточное финансирование для обеспечения информационной безопасности страны и вовсе отсутствие грамотных специалистов, способных обеспечить эту безопасность;

недостаточная экономическая способность государства;

недостаточный контроль развития информационного рынка государства;

недостаточное развитие и разработка нормативно правовой базы, регулирующей отношения в информационной сфере;

плачевное состояние промышленных отраслей государства.

Рассмотрим методы предотвращения информационных войн на уровне государства. При стремительном развитии информационного потока, информация способна быть не только положительного характера, но и отрицательного.

Угрозы и атаки при информационных войнах, для государства могут стать критически опасными, как для устойчивости государства на мировой арене, так и для состояния и поведения населения в целом. Именно поэтому информационной безопасности страны уделяется особое внимание. В первую очередь, важным является: мгновенное предотвращение и нейтрализация любой деятельности, с использованием информационных технологий, службами или даже отдельными лицами других государств, которая способна нанести ущерб национальной безопасности страны; пресечение внедрения пропаганды экстремистской идеологии и ксенофобии; развитие технологий, по обнаружению и предупреждения информационных атак; повышение устойчивости информационной инфраструктуры и ее защищенности; усиление защиты секретной информации и государственных тайн. При соблюдении данных критериев возможно предотвратить развитие военных конфликтов, которые могли вызваться посредством информационной войны.

Показатели статистики информационных атак в России за настоящий год превышают прошлые показатели. Например, атаки на автоматизированные системы управления в России за 2022 год взлетело на 80%.

Лидирующие области, которые были подвержены информационным атакам в 2022 году стали: госучреждения 16%, медицинские учреждения 11%, промышленность 8%. Объектами данных атак на первом месте оказались компьютеры, серверы и сетевое оборудование, на втором месте – люди и на третьем – веб-ресурсы. Наиболее часто применяемыми методами стали: в первую очередь – социальная инженерия, во вторую – использование вредоносного программного обеспечения и в третью – эксплуатация уязвимостей.

Последствиями, атак стали: утечка конфиденциальной информации, нарушение основной деятельности, прямые финансовые потери, ущерб интересам государства и использование ресурсов компании или частных лиц для проведения атак. Главной целью в информационных войнах и их атаках на 2022 год является получение конфиденциальной информации с помощью вредоносного программного обеспечения. Так, злоумышленники в первую очередь за первые 2 квартала 2022 года заинтересовались учетными данными пользователей VPN-сервисов. Похищение данных частных лиц прошло успешно в 21% проведенных атаках.

Таким образом, главный объект в информационных войнах – это в первую очередь сознание человека, его психологическое состояние и поведение. А ее целью является внедрение и убеждение в правильности и актуальности информации приводимых оппоненту, а также получение данных или секретной информации. Информационные атаки необходимо уметь выявлять и предотвращать, это относится как отдельно к личности, так и к

группе лиц. Информационная защита обязана развиваться в разы быстрее, чем вся индустрия информационных войн, иначе мировых катастроф не избежать.

Абашкина Алиса Юрьевна
Яковлева Светлана Сергеевна
Поволжский государственный университет телекоммуникаций и информатики,
г. Самара, Россия

Abashkina A. Yu.
Yakovleva S. S.
Povolzhsky State University of Telecommunications and Informatics,
Samara, Russia

УДК 004

ДИНАМИЧЕСКОЕ УПРАВЛЕНИЕ РЕСУРСАМИ КИБЕРБЕЗОПАСНОСТИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Ж.К. Алимсеитова, Б.С. Ахметов

DYNAMIC RESOURCE MANAGEMENT OF CYBER SECURITY OF INFORMATION OBJECTS

Zh.K. Alimseitova, B.S. Akhmetov

Аннотация. Рассматриваются вопросы повышения уровня защищенности объектов информатизации за счет оптимального распределения ресурсов защиты информации между объектами защиты с учетом действий злоумышленника. Полученные результаты и методология исследования могут быть использованы другими организациями для оптимального распределения ресурсов защиты информации между объектами защиты с учетом действий злоумышленника с целью повышения уровня защищенности объекта информатизации.

Ключевые слова: информационная безопасность, кибернетическая безопасность, защита информации, объект информатизации, объект защиты.

Abstract. The issues of increasing the level of security of informatization objects due to the optimal distribution of information protection resources between the objects of protection, taking into account the actions of an intruder, are considered. The results obtained and the methodology of the study can be used by other organizations for the optimal distribution of information