DOI: 10.58168/CISMP2024_179-181
УДК 004.9

СИСТЕМНЫЙ АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ ВОЙНЫ

К.В. Шабунина

ФГБОУ ВО «Воронежский государственный лесотехнический университет имени Г.Ф. Морозова»

Аннотация. В данной статье рассмотрено понятие «информационной войны», ее последствия и возможность ей противодействовать. При помощи системного анализа выявлены возможные угрозы, представлены методы по их устранению и, по результатам опроса, построена диаграмма последствий от кибератак, с которыми сталкиваются предприятия.

Актуальность темы обусловлена обострением геополитической обстановки, активной цифровизацией всех сфер деятельности и влиянием средств массовой информации на людей.

Ключевые слова: системный анализ, информационная война, угроза, интернет, безопасность, защита.

SYSTEMATIC ANALYSIS OF INFORMATION WARFARE THREATS

K.V. Shabunina

Voronezh State University of Forestry and Technologies named after G.F. Morozov

Abstract. This article examines the concept of "information warfare", its consequences and the possibility of countering it. With the help of a system analysis, possible threats are identified, methods for their elimination are presented and, according to the results of the survey, a diagram of the consequences of cyber attacks faced by enterprises is constructed.

The relevance of the topic is due to the aggravation of the geopolitical situation, the active digitalization of all spheres of activity and the influence of mass media on people.

Keywords: System analysis, information warfare, threat, Internet, security, protection.

Киберпространство несет огромную пользу для человечества. Доступ к любой информации в мире, получение образования на дистанционной основе, оплата товаров при помощи виртуальных средств, общение пользователей из разных городов и стран возможны благодаря сети «Интернет».

Вместе с преимуществами использования цифровых технологий выступают и недостатки. В связи с общедоступностью интернета для каждого человека в мире, его начали использовать, как оружие.

Такое понятие, как «информационная война», стало массовой и серьезной проблемой, которая касается каждого пользователя сети «Интернет.

В 1985 году впервые был введен термин «информационная война», произошло это в Китае. Первичные знания в области информационного

противостояния были заложены древнекитайским военным деятелем Сунь-цзы. Он первым привел аргументы о важности оказания информационного давления на противника.

Информационная война – это коммуникативное воздействие при помощи электронных средств.

Одной из составляющих информационной войны является – дезинформация.

Дезинформация – это умышленное распространение фальсифицированной информации, для создания обманчивой обстановки в какой-либо глобальной или локальной ситуации. Целью дезинформации является – побуждение к неверному принятию решения, выгодному дезинформирующей стороне, и распространение паники среди населения.

«Фальшивые новости в эпоху широкомасштабного распространения цифровых технологий могут нанести гораздо больший урон, чем снаряды и ракеты». Из выступления президента Болгарии Румена Радева на Всемирном конгрессе информационных агентств в Софии в июне 2019 г.

Одним из современных примеров информационной войны можно считать арабо-израильскую войну. Разногласие сторон является всемирной проблемой, так как информационная война ведется не только на территории Палестины и Израиля. Более десяти стран мира страдает из-за данного конфликта.

Защита от психологического воздействия информационной войны – сложнее, чем может показаться на первый взгляд. Общих решений защиты не существует, но могут применяться такие варианты:

- разоблачение ложной информации;
- пользование только проверенными источниками;
- патриотическое воспитание молодежи;
- контроль интернета при помощи системы «Firewall».

Примером страны, использующей систему «Firewall» для ограничения пользователей от потенциально опасной информации, является Китай. Данный проект, именуемый, как «Золотой щит», фильтрует всю информацию, попадающую в интернет. Фильтрация происходит по недопустимым ключевым словам. «Великий китайский файрвол» ограничивает доступ к определенному списку иностранных сайтов.

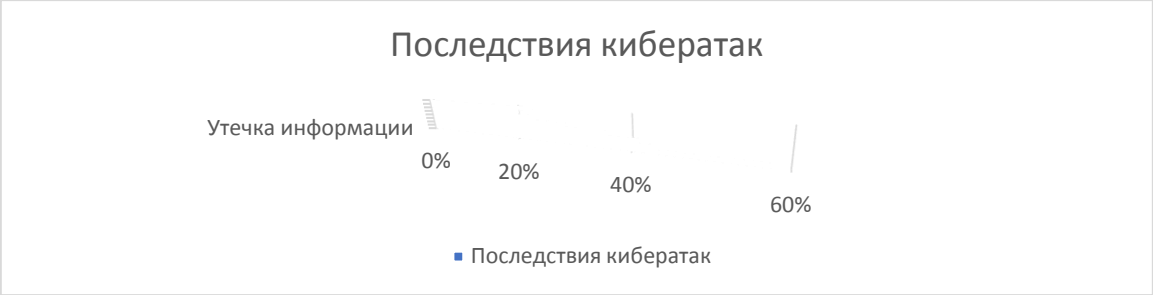
Значимую роль в информационных войнах играют кибератаки. При помощи них происходит утечка информации, нарушение ее целостности, полное уничтожение информации и сбой систем.

Кибератаки – это противоправные действия, совершаемые в цифровом пространстве при помощи телекоммуникационных средств.

Целью кибератак является нанесение вреда, получение несанкционированного доступа к информации или нарушение работы компьютерных систем.

Кибератаки несут за собой определенные последствия. На представленной далее диаграмме обозначены некоторые из них. Диаграмма

отображает, какие последствия встречаются в различных компаниях чаще всего.



Для того чтобы избежать попадания в систему злоумышленников и не допустить нанесения ущерба, необходимо иметь надежную защиту. Защита должна включать в себя несколько методов и средств защиты информации.

Самыми распространенными способами защиты информации являются – надежные пароли, установка антивирусных программ и создание резервных копий, хранимых системой, данных.

Список литературы

1. Полуэктов А.В., Макаренко Ф.В., Ягодкин А.С. Использование сторонних библиотек при написании программ для обработки статистических данных // Моделирование систем и процессов. – 2022. – Т. 15, № 2. – С. 33–41.

2. Тертерян А.С., Бровко А.В. Методы оптимизации в многокритериальных задачах с использованием локальной качественной важности критериев// Моделирование систем и процессов. – 2022. – Т. 15, № 1. – С. 107–114.

3. Хрящев, В.В. Эффективность внедрения одноранговой распределенной системы хранения и обработки защищаемой информации (TheOoL Project) / В.В. Хрящев, А.В. Ненашев // Моделирование систем и процессов. – 2021. – Т. 14, № 3. – С. 82–89. – DOI: 10.12737/2219–0767–2021–14–3–82–89.

References

1. Poluektov A.V., Makarenko F.V., Yagodkin A.S. The use of third-party libraries when writing programs for processing statistical data // Modeling of systems and processes. - 2022. – Vol. 15, No. 2. – pp. 33-41.

2. Terteryan A.S., Brovko A.V. Optimization methods in multi-criteria problems using local qualitative importance of criteria// Modeling of systems and processes. - 2022. – Vol. 15, No. 1. – pp. 107-114.

3. Khryashchev, V.V. The effectiveness of implementing a peer-to-peer distributed system for storing and processing protected information (TheOoL Project) / V.V. Khryashchev, A.V. Nenashev // Modeling of systems and processes. - 2021. – Vol. 14, No. 3. – pp. 82-89. – DOI: 10.12737/2219-0767-2021-14-3-8