Перевертун Д.Р. Психологические аспекты кибербезопасности
// Международный журнал информационных технологий и энергоэффективности.– 2024. –
Т. 9 № 4(42) с. 95–99

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

# ПСИХОЛОГИЧЕСКИЕ АСПЕКТЫ КИБЕРБЕЗОПАСНОСТИ

**Перевертун Д.Р.**
*ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: danilaperevertun@gmail.com*

**В статье рассматриваются психологические аспекты кибербезопасности, подчёркивая значимость человеческого фактора в предотвращении киберугроз. Анализируется влияние доверия, восприятия риска, эмоциональных реакций и мотивации на поведение пользователей в сети. Освещаются стратегии повышения осведомлённости и обучения, направленные на формирование защитного поведения и культуры кибербезопасности в организациях и среди индивидов. Подчёркивается важность интеграции психологических принципов в разработку и внедрение мер кибербезопасности, а также обозначается роль социальной инженерии и эмоциональной уязвимости в контексте киберугроз.**

Ключевые слова: Кибербезопасность, человеческий фактор, психологические аспекты, доверие в интернете, восприятие риска, эмоциональная уязвимость, мотивация защиты, обучение кибербезопасности, социальная инженерия, культура безопасности.

# PSYCHOLOGICAL ASPECTS OF CYBERSECURITY

**Perevertun D.R.**
*ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: danilaperevertun@gmail.com*

**The article examines the psychological aspects of cybersecurity, emphasizing the importance of the human factor in preventing cyber threats. The influence of trust, risk perception, emotional reactions and motivation on the behavior of users on the network is analyzed. Awareness-raising and training strategies aimed at developing protective behavior and a culture of cybersecurity in organizations and among individuals are highlighted. The importance of integrating psychological principles into the development and implementation of cybersecurity measures is emphasized, as well as the role of social engineering and emotional vulnerability in the context of cyber threats.**

Keywords: Cybersecurity, human factor, psychological aspects, trust on the Internet, risk perception, emotional vulnerability, protection motivation, cybersecurity training, social engineering, security culture.

В эпоху цифровизации, когда технологии проникают в каждую сферу человеческой жизни, вопросы кибербезопасности становятся всё более актуальными. Однако, несмотря на техническую оснащённость и продвинутые методы защиты, человеческий фактор остаётся самым слабым звеном в цепи кибербезопасности. В этой статье мы рассмотрим психологические аспекты, лежащие в основе кибербезопасности, а также исследуем, как

понимание человеческой психологии может способствовать повышению уровня защищённости в информационном пространстве.

Одним из ключевых психологических аспектов в контексте кибербезопасности является принцип доверия. Человек по своей природе склонен доверять системам, процессам и другим людям. Мошенники и киберпреступники активно используют этот аспект, применяя социальную инженерию и фишинг для обмана жертв.[4] Важно понимать, что доверие в цифровом мире должно быть обоснованным и проверенным.

Следующий важный аспект — это восприятие риска. Многие пользователи не осознают реальной угрозы, которую представляют кибератаки, либо, наоборот, переоценивают свои способности к защите. Это приводит к тому, что меры безопасности либо игнорируются, либо применяются некорректно. Обучение и повышение осведомлённости могут сыграть ключевую роль в изменении этой ситуации.

В понимании психологических аспектов угроз кибербезопасности ключевую роль играет осознание того, что за каждым действием в сети стоит человек со своими убеждениями, страхами, ожиданиями и предрассудками. Эти индивидуальные характеристики в комплексе влияют на уровень уязвимости перед лицом киберугроз. Принцип доверия, например, является фундаментальным в построении межличностных отношений и взаимодействия с технологиями.[2] Однако в контексте кибербезопасности это доверие может быть использовано против человека. Мошенники и хакеры активно эксплуатируют доверчивость, прибегая к таким методам, как социальная инженерия и фишинг, чтобы манипулировать жертвами и выманивать у них конфиденциальную информацию.

Восприятие риска также играет существенную роль в том, как индивиды оценивают потенциальную угрозу своей кибербезопасности. Некоторые могут недооценивать риск, полагая, что они не представляют интереса для злоумышленников, или же переоценить свои способности защитить себя, что приводит к избыточной самоуверенности и игнорированию базовых мер безопасности. Эта дихотомия в восприятии угроз создаёт условия, при которых пользователи могут стать лёгкой добычей для киберпреступников.

Не менее важен эмоциональный аспект, включающий в себя такие чувства, как страх, жадность или чувство непобедимости. Эти эмоции могут облегчить злоумышленникам задачу манипулирования своими жертвами. Например, страх потери может побудить человека к поспешным действиям, таким как нажатие на вредоносную ссылку или предоставление конфиденциальных данных, если злоумышленник убедит его, что это необходимо для предотвращения ещё больших потерь.[7] Жадность может быть использована при различных схемах обмана, обещающих большую прибыль за минимальные усилия или вложения.

Таким образом, психологические аспекты угроз кибербезопасности заключаются в сложном взаимодействии между индивидуальными особенностями личности, её эмоциональным состоянием и способностью критически оценивать информацию и риски. Разумеется, эти аспекты не существуют в вакууме и взаимодействуют с техническими и социальными факторами, создавая сложную картину угроз и вызовов в области кибербезопасности.[5] В этой связи, понимание и учёт психологических аспектов могут значительно повысить эффективность предотвращения киберугроз и формирования культуры кибербезопасности как в организациях, так и среди индивидуальных пользователей. Осознание того, как эмоции и психологические настройки влияют на принятие решений в сети, может помочь в разработке более интуитивно понятных и пользовательски

ориентированных систем безопасности, которые учитывают человеческие слабости и стараются минимизировать их влияние.

Понимание психологии не только помогает выявить слабые места в защите, но и разработать более эффективные методы противодействия киберугрозам. К примеру, использование геймификации в процессах обучения может значительно повысить интерес и вовлечённость сотрудников в изучение вопросов кибербезопасности.

Мотивация является ключевым элементом в обеспечении кибербезопасности. Создание системы поощрений за соблюдение правил и протоколов безопасности может стимулировать более ответственное поведение пользователей и сотрудников.

В сфере кибербезопасности психология защиты занимает центральное место, исследуя, как человеческие факторы влияют на принятие и эффективность мер безопасности. Понимание того, что стоит за решением человека следовать или игнорировать рекомендации по кибербезопасности, может пролить свет на способы укрепления защитных механизмов в информационном пространстве. На уровне организаций и индивидов развитие защитного поведения в цифровом мире часто зависит от сложного взаимодействия между осознанием угрозы, восприятием собственной уязвимости и мотивацией к действию.

Защитное поведение в контексте кибербезопасности не сводится лишь к техническим навыкам и знаниям. Оно глубоко укоренено в психологических мотивациях и отношениях, влияющих на то, как люди воспринимают свою способность влиять на безопасность собственных данных и систем.[6] Это включает в себя уровень самоэффективности, то есть веры в свои способности осуществлять необходимые действия для защиты от киберугроз. Люди с высоким уровнем самоэффективности склонны активнее принимать меры по обеспечению кибербезопасности, поскольку они уверены в своих способностях успешно применять необходимые инструменты и стратегии.

Ключевым элементом психологии защиты является также мотивация к изменению и поддержанию безопасного поведения в интернете. Эта мотивация может быть усилена через различные стратегии, включая обучение, осведомлённость о рисках и последствиях кибератак, а также через системы поощрений и наказаний в организационной культуре. Понимание того, что действия индивида имеют значение и могут защитить как личные данные, так и корпоративные активы, способствует формированию глубоко укоренённого чувства ответственности и заинтересованности в кибербезопасности.

Помимо мотивации и самоэффективности, важную роль в психологии защиты играет и образовательный компонент. Обучение и повышение осведомленности не только передают необходимые знания и навыки, но и способствуют формированию правильного восприятия киберугроз и понимания ценности проактивного подхода к безопасности.[3] Информационные кампании и образовательные программы, направленные на развитие критического мышления и осознанного отношения к киберрискам, являются неотъемлемой частью стратегии защиты.

Психологические аспекты кибербезопасности играют ключевую роль в формировании эффективной стратегии защиты информационных систем и данных. Понимание того, как человеческий фактор влияет на безопасность, позволяет разработать более целенаправленные и эффективные подходы к её обеспечению.

Внедрение психологических знаний в практику кибербезопасности охватывает не только разработку технических решений, но и формирование корпоративной культуры, обучение и

повышение осведомлённости среди пользователей. Программы обучения должны быть направлены не только на передачу знаний о технических аспектах безопасности, но и на развитие критического мышления, способности оценивать риски и принимать обоснованные решения в условиях неопределённости.

Следует также обратить внимание на социально-психологические аспекты, такие как формирование доверия внутри организации, управление конфиденциальностью и приватностью, а также на механизмы противодействия социальной инженерии и манипуляциям. Инвестирование в развитие социального капитала и построение открытой, взаимоподдерживающей обстановки в коллективе может существенно повысить уровень кибербезопасности.

Необходимо также учитывать влияние новых технологий, таких как искусственный интеллект и машинное обучение, на психологические аспекты кибербезопасности. Автоматизация и применение алгоритмов для предотвращения кибератак может с одной стороны уменьшить человеческий фактор как источник угроз, но с другой — создать иллюзию полной безопасности, что также может быть рискованным.

Стоит подчеркнуть, что человеческий фактор играет критически важную роль в обеспечении защиты в цифровой эпохе. Понимание того, как психологические характеристики и поведенческие тенденции влияют на безопасность информационных систем, позволяет формировать более эффективные и адаптированные подходы к защите от киберугроз. Важность разработки и реализации образовательных программ, направленных на повышение осведомленности и обучение безопасному поведению в интернете, не может быть переоценена. Такие программы должны учитывать психологические аспекты восприятия риска, доверия, эмоционального вовлечения и мотивации к защите, чтобы стимулировать формирование устойчивой культуры кибербезопасности среди пользователей и в организациях.

Кроме того, необходимо акцентировать внимание на том, что кибербезопасность — это не статичная дисциплина, а динамично развивающаяся область, требующая постоянной адаптации к новым угрозам и технологическим реалиям.[1] В этом контексте понимание психологических основ поведения пользователей и злоумышленников становится критически важным для предотвращения киберинцидентов и минимизации их последствий. Эффективная стратегия кибербезопасности должна включать в себя не только технические решения, но и активное участие пользователей, основанное на глубоком понимании психологических аспектов их взаимодействия с цифровым миром.

В заключение, интеграция психологических знаний в практику кибербезопасности открывает новые горизонты для разработки более эффективных методов защиты, обучения и профилактики киберугроз. Взаимодействие между техническими и человеческими аспектами безопасности должно стать основой для создания устойчивых и адаптируемых систем защиты в информационном обществе будущего.

**Список литературы**

1. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – С. 1-6.

2. Гельфанд А. М. и др. Интернет вещей (IoT): Угрозы безопасности и конфиденциальности//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 215-220.
3. Гельфанд А. М. и др. Исследование распределенного механизма безопасности для устройств интернета вещей с ограниченными ресурсами//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 321-326.
4. Косов Н. А. и др. Анализ методов машинного обучения для детектирования аномалий в сетевом трафике//Цифровизация образования: теоретические и прикладные исследования современной науки. – 2021. – С. 33-37.
5. Косов Н. А., Тимофеев Р. С. Сравнение методов обучения свёрточных нейронных сетей//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 526-530.
6. Косов Н.А., Мазепин П.С., Гришин Н.А. Применение нейронных сетей для автоматизации тестирования программного обеспечения //Наукосфера. – 2020. – №. 6. – С. 152-156.
7. Штеренберг С.И. Методика построения защищенных систем искусственного интеллекта для проведения электроретинографии в офтальмологии //Офтальмохирургия. – 2022. – №. 4s. – С. 51-57.

**References**

1. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – pp. 1-6.
2. Gelfand A.M. et al. Internet of things (IoT): security and privacy threats//Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 215-220.
3. Gelfand A.M. et al. Investigation of a distributed security mechanism for Internet of Things devices with limited resources //Actual problems of infotelecommunications in science and education (APINO 2020). – 2020. – pp. 321-326.
4. Kosov N. A. et al. Analysis of machine learning methods for detecting anomalies in network traffic //Digitalization of education: theoretical and applied research of modern science. – 2021. – pp. 33-37.
5. Kosov N.A., Timofeev R.S. Comparison of training methods for convolutional neural networks//Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 526-530.
6. KOSOV N.A., MAZEPIN P.S., GRISHIN N.A. Application of neural networks for software testing automation //The sciencosphere. - 2020. – No. 6. – pp. 152-156.
7. Shterenberg S. I. Methods of constructing protected artificial intelligence systems for conducting electroretinography in ophthalmology //OPHTHALMOSURGERY. – 2022. – No. 4s. – pp. 51-57.