КИБЕРБЕЗОПАСНОСТЬ СОВРЕМЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМ: ПРОБЛЕМЫ И ПУТИ РЕШЕНИЯ

Халилов Султанбек Замирович
Студент бакалавриата, Факультет компьютерных наук,
Нукусский государственный технический университет,
Нукус, Узбекистан
hsultanbek42@gmail.com

Аннотация: В данной работе проводится комплексный анализ состояния информационной безопасности в условиях глобальной цифровизации. В статье приводится актуальная статистика кибератак, исследуются современные угрозы, такие как целевые атаки (APT) и программы-вымогатели, а также подчеркивается критическая роль «человеческого фактора» в обеспечении устойчивости систем. Особое внимание уделено перспективным методам защиты: архитектуре «нулевого доверия» (Zero Trust) и внедрению технологий искусственного интеллекта. В результате исследования сделан вывод о необходимости синергии технологических решений и формирования культуры цифровой гигиены как единственно эффективного способа противодействия современным киберугрозам.
Ключевые слова: кибербезопасность, информационные системы, социальная инженерия, искусственный интеллект, цифровая грамотность.

Введение

В эпоху тотальной цифровизации компьютерные системы стали фундаментом жизнедеятельности общества. От стабильности их работы зависит не только комфорт граждан, но и функционирование государственных институтов и финансовых рынков. В самом широком смысле кибербезопасность представляет собой стратегическое направление информационной безопасности, сфокусированное на защите компьютерных сетей, программ и массивов данных от несанкционированного доступа, деструктивного вмешательства или уничтожения. Фундаментальная цель этой дисциплины заключается в поддержании трех базовых принципов: конфиденциальности, целостности и доступности информации. Конфиденциальность гарантирует, что сведения остаются доступными исключительно авторизованным лицам; целостность обеспечивает защиту данных от скрытого искажения или подделки; а доступность подразумевает стабильное и бесперебойное функционирование ресурсов для легитимных пользователей. Именно на сохранении этого баланса строится вся архитектура защиты современных систем. [3]

Однако стремительный технологический прогресс породил и новые риски: киберпреступность превратилась в высокодоходную индустрию, а методы атак становятся всё более изощренными. Тезис данной работы заключается в том, что

эффективная кибербезопасность сегодня — это не просто набор технических средств, а многоуровневая стратегия, сочетающая технологические инновации и цифровую грамотность пользователей.

Основная часть

Масштабы угроз в глобальном киберпространстве наглядно подтверждаются статистическими данными. Исследования показывают стремительную динамику роста интенсивности атак: если в 2019 году нападения на информационные ресурсы происходили в среднем каждые 15 секунд, то уже к 2021 году этот интервал сократился до 12 секунд. Результатом такой активности становятся беспрецедентные утечки данных — только за один 2019 год в открытый доступ попало более 14 миллиардов записей, содержащих конфиденциальную информацию. Эти цифры подчеркивают, что киберпреступность превратилась в глобальный вызов, требующий немедленной реакции. [1]

Одной из центральных проблем современной кибербезопасности является качественное изменение характера угроз. На смену массовым и сравнительно простым вирусам пришли целевые атаки (APT-угрозы), которые годами могут оставаться незамеченными внутри защищенного периметра. Особую опасность представляют программы-вымогатели, блокирующие работу целых корпораций, и использование искусственного интеллекта для создания фишинговых сообщений, которые практически невозможно отличить от реальных. Ситуация осложняется размытием самого «периметра» защиты: развитие облачных технологий и удаленной работы привело к тому, что классические антивирусы и файерволы больше не обеспечивают полной безопасности, так как данные и пользователи теперь находятся вне стен офиса.

Другим критическим фактором остается «человеческий фактор». Технологические системы защиты могут быть сколь угодно совершенными, но они оказываются бессильны перед методами социальной инженерии. Ошибки сотрудников, пренебрежение правилами цифровой гигиены и использование слабых паролей открывают злоумышленникам прямой доступ к конфиденциальной информации. Таким образом, проблема безопасности современных систем лежит не столько в области программного кода, сколько в области психологии и организационной культуры.

Для практической реализации фундаментальных принципов кибербезопасности применяется широкий спектр технических методов. Обеспечение конфиденциальности базируется на использовании криптографических протоколов шифрования данных и строгом контроле прав доступа, что исключает возможность прочтения информации посторонними лицами. Поддержание целостности системы достигается через внедрение алгоритмов хеширования, регулярный мониторинг изменений в реальном времени и создание резервных копий (бэкапов), позволяющих восстановить эталонное состояние данных в случае их повреждения. Наконец, принцип доступности реализуется за счет создания отказоустойчивых систем и

резервирования аппаратных мощностей, что гарантирует стабильную работу информационных ресурсов даже в условиях технических сбоев или внешнего воздействия. Совокупность этих инструментов формирует первый эшелон защиты любой современной компьютерной системы. [4]

Решение этих проблем требует комплексного перехода к новым моделям защиты. Одной из наиболее перспективных является архитектура «нулевого доверия» (Zero Trust), подразумевающая, что ни один пользователь или устройство внутри сети не считается доверенным по умолчанию. Каждое действие требует постоянной верификации. Параллельно с этим необходимо внедрение систем на базе машинного обучения, способных в реальном времени анализировать аномалии в поведении трафика и предотвращать атаку еще на стадии ее зарождения. Однако технические средства должны обязательно дополняться правовыми механизмами и непрерывным обучением кадров, что позволит создать многоуровневый барьер на пути киберпреступников.

Таким образом, противодействие современным вызовам требует не фрагментарных мер, а системного взаимодействия на уровне организаций, государств и гражданского общества. Повышение уровня кибербезопасности невозможно без реализации комплекса практических шагов: от регулярного обновления программного обеспечения и внедрения многофакторной аутентификации до масштабных инвестиций в защитные технологии. При этом критически важным остается обучение пользователей основам безопасности, так как в условиях постоянно меняющегося ландшафта угроз защита цифровой среды становится общей ответственностью. Только через синергию технологических решений и осознанной цифровой дисциплины можно сформировать устойчивую и безопасную экосистему для всех участников. [2]

Заключение

Подводя итог, можно утверждать, что кибербезопасность современных компьютерных систем — это непрерывный процесс, а не конечный результат. В условиях, когда технологии взлома развиваются параллельно со средствами защиты, единственным эффективным решением является проактивный подход. Необходимо сочетать инновационные технологические решения (такие как ИИ и архитектура Zero Trust) с повышением цифровой грамотности на всех уровнях. Будущее информационной безопасности зависит от способности общества адаптироваться к новым вызовам и рассматривать защиту данных как неотъемлемый элемент общей культуры использования современных технологий.

ЛИТЕРАТУРА:

1. Наиля Рашидовна Шевко, Сергей Яковлевич Казанцев КИБЕРБЕЗОПАСНОСТЬ: ПРОБЛЕМЫ И ПУТИ РЕШЕНИЯ // Вестник экономической безопасности. 2020. №5. URL: https://cyberleninka.ru/article/n/kiberbezopasnost-problemy-i-puti-resheniya

2. Ерастов Е. Д. СОВРЕМЕННЫЕ ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ: ВЫЗОВЫ И РЕШЕНИЯ // Вестник науки. 2024. №10 (79). URL: https://cyberleninka.ru/article/n/sovremennye-problemy-kiberbezopasnosti-vyzovy-i-resheniya

3. Сотников, Д. П. Решение вопросов кибербезопасности в современных компаниях / Д. П. Сотников. — Текст: непосредственный // Молодой ученый. — 2024. — № 21 (520). — С. 339-341. — URL: https://moluch.ru/archive/520/114403.

4. Шаханов Г., Дурдыев Б., Назаров Т., Вепаев Ш. КИБЕРБЕЗОПАСНОСТЬ И МЕТОДИКИ БОРЬБЫ В МИРЕ // Символ науки. 2024. №2-2-2. URL: https://cyberleninka.ru/article/n/kiberbezopasnost-i-metodiki-borby-v-mire