ЦИФРОВОЕ ПРОСТРАНСТВО И ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Капустина Д.Д., Борисенко Р.С.
Научный руководитель: ст. преподаватель Ковалькова И.А.
Белорусский национальный технический университет

Современные технологические достижения значительно продвинули общество, проникая в различные аспекты повседневной жизни, создавая новое цифровое пространство. Наряду с инновационными отношениями усилия по цифровизации создают риски, влияющие на вопросы конфиденциальности и защиты индивидуальной информации.

Проблема обеспечения безопасности информации рассматривается странами мира, а также отдельными предприятиями. Информационная безопасность является важной частью информационной культуры человека.

Цифровое пространство как цифровая среда – «среда логических объектов, используемая для описания (моделирования) других сред (в частности, электронной и социальной) на основе математических законов» [1] создает проблему цифрового неравенства и проблему контроля цифровой власти, что означает ответственность за различные аспекты жизни. Поскольку развитие сети диктует базовое управление коллективными действиями, создание сложных, взаимосвязанных систем, таких как защита важнейших национальных ресурсов, требует киберпространства. [2] Технической информации недостаточно. Для полного понимания тем защиты данных необходим дополнительный контекст. Поэтому роль человека в кибербезопасности всеобъемлюща. [3]

Угрозы информационной безопасности следует разделить по таким критериям, как например, по цели атаки, методу или по типу атакуемого ресурса. К наиболее известным видам угроз относятся: вредоносное ПО (вирусы, трояны, черви и другие вредоносные программы), фишинг (мошеннические действия, направленные на получение конфиденциальной информации путем отправки писем или сообщений), сетевые атаки (атаки, направленные на нарушение работы сети), уязвимости ПО (злоумышленники применяют методы обхода систем безопасности, например, путем использования украденных учетных данных или подмены лиц).

Проблемы информационной безопасности – наиболее обсуждаемая тема наших дней, а новые методы атак формируются ежедневно – всех следует следить за последними новостями в области информационной безопасности и не забывать о том, чтобы своевременно обновлять системы защиты.

Для борьбы с угрозами информационной безопасности необходимо использовать комплексный подход.

Таблица 1

Способы решения проблем информационной безопасности		
Защита	Мониторинг	Реагирование на инциденты
- установка антивирусного ПО и брандмауэров	- следить за сетевым трафиком и активностью пользователей	- планировать варианты реагирования на инциденты
- активно обновлять ПО		
- использовать сложные пароли и минимум двухфакторную аутентификацию	- пользоваться системами обнаружения вторжений и предотвращения вторжений	- оперативно реагировать на действия, вызывающие подозрения
- обучать сотрудников тонкостям информационной безопасности		
- шифровать данные	- анализируйте журналы безопасности	- восстановление систем после инцидента

Кроме перечисленных мер, нужно помнить о незамедлительном усовершенствовании системы информационной безопасности. Обязательно проводить оценку рисков и внедрять новые методы защиты. Только многоуровневый подход к безопасности позволит минимизировать риски и защитить информацию.

В современных условиях цифровизации информационного общества существуют риски кражи личных данных. Компании, имеющие у себя персональную и финансовую информацию клиентов, как правило, вероятнее всего подвержены хакерским атакам.

В связи с этим, особое внимание следует уделить обучению персонала. Сотрудники должны быть осведомлены о современных методах социальной инженерии и фишинга, а также о правилах безопасной работы с информацией, включая использование сильных паролей, соблюдение политики доступа и своевременное обновление программного обеспечения. Регулярные тренинги и симуляции кибератак помогут повысить бдительность и эффективность защиты от внутренних и внешних угроз, сделав систему безопасности комплексной и надежной.

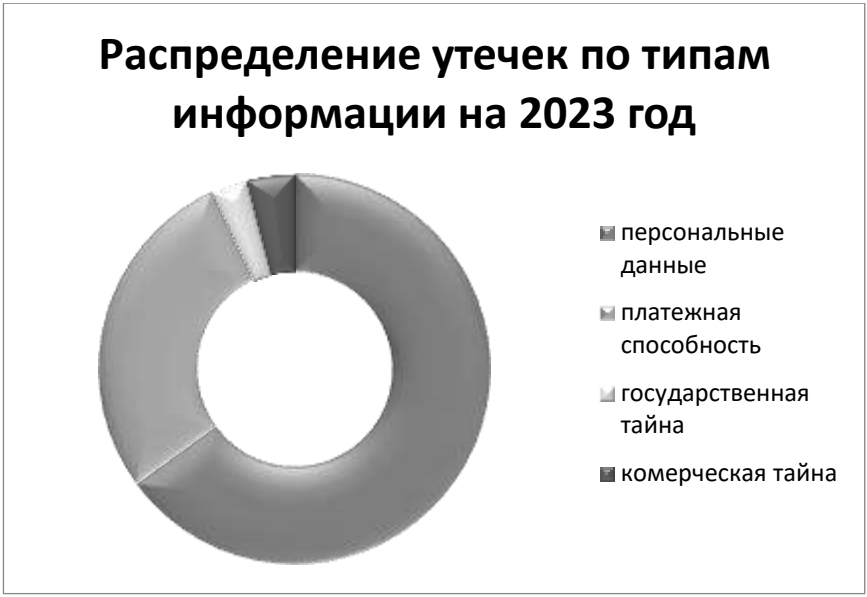

Рисунок 2. Распределение утечек по типам информации на 2023 год

Таким образом, опираясь на исследование, можно заключить, что в мире, где преобладает цифровое пространство, пути решения найденных угроз и проблем, возможно, заключаются в развитии способности противостояния современным угрозам. В данном случае это стратегическое мышление, развитие возможностей, создание и образование, обучение, кооперацию и взаимодействие субъектов обеспечения информационной безопасности с учетом человеческого фактора.

Литература

1. ГОСТ Р 52292–2004. Информационная технология. Электронный обмен информацией.

2. Курылев К.Л., Цаканян В.Т. Цифровая зависимость НАТО // Вестник Московского государственного областного университета. Серия: История и политические науки. – 2018. − №1. − С.45-51.

3. Кибербезопасность: человеческий фактор, 12.06.2018 [Электронный ресурс]. URL: https://legal-it.club/kiberbezopasnost-chelovecheskij-faktor (дата обращения: 11.11.2024).