ЧТО ТАКОЕ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ? ЕЁ РОЛЬ В СОВРЕМЕННОМ МИРЕ

Коннов Михаил Александрович

студент, кафедры информационно вычислительные комплексы, Ульяновский Государственный Технический Университет, РФ, г. Ульяновск

Игнатьев Дмитрий Сергеевич

студент, кафедры информационно вычислительные комплексы, Ульяновский Государственный Технический Университет, РФ, г. Ульяновск

Зотов Глеб Владиславович

студент, кафедры информационно вычислительные комплексы, Ульяновский Государственный Технический Университет, РФ, г. Ульяновск

Кадырова Динара Руслановна

студент, кафедры информационно вычислительные комплексы, Ульяновский Государственный Технический Университет, РФ, г. Ульяновск

Лушников Леонид Леонидович

студент, кафедры информационно вычислительные комплексы, Ульяновский Государственный Технический Университет, РФ, г. Ульяновск

Тамьярова Майя Владиславовна

научный руководитель, канд. техн. наук, Ульяновский Государственный Технический Университет, РФ, г. Ульяновск

Аннотация. В статье рассматриваются актуальные вопросы в области информационной безопасности в условиях цифровизации экономики. Современная политика в данной области является следствием сложности, многофакторности и масштабности развития информационного общества. При этом финансовый сектор связан непосредственно с денежными потоками, что делает его особенно уязвимым для злоумышленников. В данной связи приобретает особую актуальность использование системы информационной безопасности, которая позволяет защищать организации финансового и коммерческого секторов от кибератак и несанкционированного использования данных.

Ключевые слова: информационная безопасность, цифровизация, цифровизация экономики, информационные технологии.

Хотя цифровой век способствовал росту и процветанию компаний, он также сделал их более уязвимыми для кибератак, особенно в условиях, когда большая часть наших повседневных действий выполняется в Интернете.

В этом смысле цифровая безопасность имеет первостепенное значение для любого бизнеса, каким бы небольшим он не был. Кибератака может нанести огромный урон организации и ее клиентам, особенно если от неё нет какой-либо защиты.

Цифровая безопасность - это широкий термин, который относится к различным формам защиты данных и информации в Интернете от кражи, повреждения или взлома [6].

Она включает в себя различные типы инструментов для защиты данных и информации, от установки брандмауэров и антивирусного программного обеспечения на компьютерах и различных аппаратных средствах до шифрования жестких дисков и использования надежных паролей.

То есть цифровая безопасность - это защита содержимого устройств, подключенных к Интернету, которые могут подвергнуться взлому, фишингу и многому другому. Иными словами, цифровая безопасность - это фундаментальная практика защиты личной информации, такой как личные или конфиденциальные данные.

Термины цифровая безопасность, информационная безопасность и кибербезопасность - это не одно и то же, но они взаимосвязаны, поскольку цифровая безопасность защищает информацию, инфраструктуру систем, их физические сети, компьютерные системы и хранимые данные от несанкционированного доступа.

Это означает, что кибербезопасность действительно является частью цифровой безопасности, и это термины, которые связаны и работают рука об руку, поскольку кибербезопасность играет роль защиты физического оборудования, в то время как цифровая безопасность выполняет важную задачу по сохранению информации, циркулирующей устройствах, от различного рода кибератак.

Персональные данные: информация, связанная с идентификацией личности, считается подверженной риску. Например, такие данные, как имя, номер телефона, адрес проживания, адрес электронной почты, IP-адрес и, в зависимости от страны, номера, относящиеся к социальному страхованию, с помощью которых можно открывать мошеннические счета по кредитным картам - это данные, которые всегда необходимо защищать. Эти персональные данные считаются представляющими опасность, поскольку обычно они включают информацию, потенциально указывающую местонахождение жертвы.

Финансовые данные: Если речь идет о транзакциях, мы можем с полной уверенностью сказать, что персональные платежные данные считаются наиболее востребованными киберпреступниками. Информация, которая включает номера кредитных и дебетовых карт (включая даты истечения срока действия и коды), номера онлайн-банков (учетная запись и маршрут) и PIN-коды - это информация, которая в конечном итоге должна быть защищена для предотвращения краж и финансового мошенничества [4].

Данные о состоянии здоровья: этот тип данных, рассматриваемых как конфиденциальные, включает в себя соответствующую информацию о здоровье людей, истории посещений врачей, лекарства и подписки на медицинское страхование. Этот тип информации представляет большой интерес для киберпреступников, поскольку у них есть возможность использовать свою медицинскую информацию для выставления ложных страховых требований или заказа и перепродажи лекарств.

Как защитить данные с помощью цифровой безопасности?

а) Ознакомление с безопасностью: во всех организациях очень важно информировать и обучать новых сотрудников и руководителей правилам безопасности, поскольку таким образом компания гарантирует, что каждый член команды будет знать, как наилучшим образом использовать различные программы и программное обеспечение.

б) Внедрение устройств безопасности: все программное и аппаратное обеспечение, которым управляет компания, должно попадать под строгие рамки безопасности, как с физической, так и с компьютерной точки зрения. Это означает, что все технологические устройства

должны иметь соответствующие антивирусные и антишпионские решения, а в идеале и платные, поскольку бесплатные решения не гарантируют раннего обнаружения и устранения вредоносных программ.

в) Безопасные облачные решения: для тех организаций, которые заключают технологические контракты со сторонними организациями типа SaaS или программного обеспечения в облаке, важно, чтобы специалист по безопасности проверял, действительно ли эти поставщики обновлены и имеют ли они все соответствующие сертификаты и стандарты защиты данных, гарантируя безопасность и конфиденциальность информации.

г) Защита данных с помощью контроля доступа: случайные или преднамеренные утечки данных встречаются чаще, чем может показаться на первый взгляд. В соответствии с исследованием, проведенным компанией Ermetic, занимающейся безопасностью облачного доступа, было выявлено, что почти 80% опрошенных компаний испытали по крайней мере одну утечку облачных данных в средах IaaS / PaaS за последние 18 месяцев.

Хоть и не существует «стопроцентного» метода предотвращения подобных рисков утечки информации, но тем не менее их можно снизить, используя многоуровневые системы контроля доступа, например использование паролей, двухэтапной или многоступенчатой аутентификации и токенов цифровой безопасности [5].

Цифровая безопасность - это быстрорастущая область, цель которой - защитить данные от взлома. Для предприятий и организаций важно принимать меры предосторожности, максимально снижая возможность получения данных при кибератаках.

Сегодня смартфоны стали одним из важнейших аспектов нашей жизни, как если бы это было нашим самым ценным земным благом. Мы путешествуем с ними, работаем, общаемся.

Кроме того, в настоящее время смартфоны быстро заменяют компьютеры в том смысле, что на них можно легко выполнять большинство задач, вместо того, чтобы носить с собой персональные компьютеры и ноутбуки.

Сравним, к примеру, смартфоны двух конкурирующих между собой компаний: Apple и Samsung, с соответствующими операционными системами: IOS и Android

Угрозы безопасности мобильных устройств на Android и iOS направлены на компрометацию или кражу конфиденциальных данных со смартфонов. Однако, похоже, нам присущи идеи или, скорее, мифы, которые полностью ложны и только наносят ущерб нашей безопасности в Интернете.

Устройства Apple на iOS более безопасны. Многие люди считают, что если у них есть устройство на iOS, то им не нужно беспокоиться о безопасности своих данных. Apple уделила большое внимание маркетингу того, насколько безопасны ее устройства и как они делают их более безопасными, нежели другие производители.

Apple использует некоторые строгие механизмы безопасности на устройствах iOS, поэтому люди не склонны беспокоиться об использовании дополнительных мер безопасности на этих устройствах.

Да, атаки на устройства iOS встречаются реже, но они все еще происходят. Как сообщает Ars Technica, исследователи нашли способ использовать чип Bluetooth в iPhone, который является ключом к работе устройства в режиме пониженного энергопотребления, и заразили его вредоносным ПО.

Список литературы:

1. Голубитченко, М. А. Особенности информационной безопасности в кредитно-финансовой сфере / М. А. Голубитченко, Е. П. Беренвальд, Е. Е. Парасюк. — Текст : непосредственный //

Молодой ученый. — 2021. — № 52 (394). — С. 9-13.

2. Информационная безопасность цифровой экономики // https://spravochnick.ru/: научный словарь справочник. URL: https://spravochnick.ru/ekonomika (дата обращения 14.01.2023)

3. Кибербезопасность, будущее и ИИ // https://www.securitylab.ru/: информационный портал. URL: https://www.securitylab.ru(дата обращения 14.01.2023)

4. Корнев, Л. В. Обеспечение информационной безопасности в условиях цифровизации / Л. В. Корнев. — Текст : непосредственный // Молодой ученый. — 2022. — № 12 (407). — С. 7-11.

5. Ковалев О. Г., Скипидаров А.А. НОРМАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ РЕАЛИЗАЦИИ СТРАТЕГИИ КИБЕРБЕЗОПАСНОСТИ В ГОСУДАРСТВАХ ЕВРОПЕЙСКОГО СОЮЗА // Столыпинский вестник. 2021. №2. URL: https://cyberleninka.ru/article/n/normativno-pravovoe-regulirovanie-realizatsii-strategii-kiberbezopasnosti-v-gosudarstvah-evropeyskogo-soyuza (дата обращения: 25.01.2023).

6. Щербакова Н.В. ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЩЕСТВА В УСЛОВИЯХ СТАНОВЛЕНИЯ ЦИФРОВОЙ ЭКОНОМИКИ // Вестник НГУЭУ. 2021. №1. URL: https://cyberleninka.ru/article/n/problemy-informatsionnoy-bezopasnosti-obschestva-v-usloviyah-stanovleniya-tsifrovoy-ekonomiki (дата обращения: 25.01.2023).