ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КОММЕРЧЕСКИХ ПРЕДПРИЯТИЯХ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

*Т.Р. Хасбулатов*

**Аннотация:** 21 век заслужено можно считать веком информационного общества, где большую роль играют информационные технологии и информационная безопасность. В настоящее время информационная безопасность имеет решающее значение для всех организаций, чтобы защитить свою информацию и вести качественно свой бизнес. Информационная безопасность определяется как защита информации и системы, а также аппаратных средств, которые используют, хранят и передают эту информацию. Существуют проблемы и риски, связанные с внедрением информационной безопасности в организации. Необходимо провести анализ проблем информационной безопасности и рассмотреть методики для выведения рекомендаций по информационной безопасности в коммерческих организациях в условиях цифровой экономики.

**Ключевые слова:** информационная безопасность, проблемы информационной безопасности, управление рисками, цифровая экономика, коммерческие организации.

**Введение.** Мы живем в мире, где информация играет основную роль в жизни общества. Информация является одним из самых важных активов организации. Для любой организации информация является ценной и, соответственно, она должна быть надлежащим образом защищена. Так как есть лица, которые законными и не очень способами стремятся эту информацию заполучить. Безопасность заключается в объединении систем, операций и внутреннего контроля для обеспечения целостности и конфиденциальности данных и процедур работы в организации.

Использование на производстве информационных технологий и программно-аппаратных средств стало обычным делом в современных предприятях.

В современных предприятиях стало обычным делом использовать на производстве информационные технологии и программно-аппаратные средства. Сегодня нельзя найти предприятие, где бы не использовалась ИТ-инфраструктура, это касается даже самой малой организации. Это означает, что организации не могут функционировать без ИТ-систем.

Кроме того, это стало крайне важным для обеспечения конкурентных преимуществ для организаций, и нет никакого способа, которым можно было бы вести бизнес без информационных технологий и систем. Мы живем в век цифровой экономики, где основную роль играют современные информационные технологии и системы. Благодаря этому стерлись границы удаленности друг от друга. Бизнесмен с одного континента может спокойно вести бизнес на другом континенте, не покидая свой дом.

С учетом вышесказанного следует отметить, что наличие ИТ в бизнесе не означает успеха или гарантированных результатов, если только организации не примут меры для обеспечения того, чтобы их протоколы и процедуры информационной безопасности были хорошо разработаны, а их ИТ-ресурсы были защищены от внешних и внутренних угроз.

В современном мире популярность получил термин «Цифровая экономика». Цифровая экономика относится к экономике, основанной на цифровых вычислительных технологиях, хотя мы все больше воспринимаем это как ведение бизнеса через рынки, основанные на всемирной паутине Интернет. Цифровая экономика также называется Интернет-экономикой, новой экономикой или веб-экономикой. Цифровая экономика все больше переплетается с традиционной экономикой, что затрудняет четкое разграничение. Цифровая экономика - одна из наиболее стремительно развивающихся отраслей во всем мире. Это важный двигатель инноваций и развития предприятий. [6]

Цифровая экономика оказала существенное влияние на розничные продажи товаров народного потребления. Одним из последствий стало быстрое распространение розничных торговцев без физического присутствия, таких как Ebay или Amazon. кроме того, традиционные розничные торговцы, такие как WalMart и Macys, реструктурировали свой бизнес, чтобы адаптироваться к цифровой экономике. Некоторые розничные торговцы, такие как Forever 21, объявили о банкротстве в результате своей неспособности предвидеть и адаптироваться к цифровой экономике. Цифровая экономика ставит вопросы информационной безопасности на первое место. [5]

История информационной безопасности начинается с истории компьютерной безопасности. Это началось примерно в 1980 году. В 1980 году использование компьютеров было сосредоточено на вычислительных центрах, где реализация компьютерной безопасности сосредотачивалась на обеспечении физической вычислительной инфраструктуры, которая являлась на тот период высокоэффективной для организации. Хотя открытость интернета позволило предприятиям быстро перенять технологическую экосистему, она также оказалась большой слабостью с точки зрения информационной безопасности. Первоначальное назначение системы как средства совместной работы между группами доверенных коллег больше не является практичным, поскольку ее использование расширилось до миллионов часто анонимных пользователей. Многочисленные инциденты по безопасности, связанные с вирусами, червями и другими вредоносными программными продуктами, произошли со времен червя Morris, который был первым и закрыл 10% систем в Интернете в 1988 году. Эти инциденты становятся все более сложными и дорогостоящими. Однако осведомленность об информационной безопасности была повышена. Многие организации внедрили системы информационной безопасности для защиты своих данных. [2]

В данной статье мы рассмотрим проблему информационной безопасности в коммерческих предприятиях в условиях цифровой экономики. Выявим ряд проблем, и предложим некоторые решения, которые будут полезны в будущем для коммерческих предприятий.

**Методология исследования.** Методология, которая использовалась для сбора данных при данном исследовании, заключается в чтении и обзоре литературы, чтобы обеспечить глубокое понимание информационной безопасности и всевозможных угроз, которые могут возникнуть в коммерческих предприятиях в условиях цифровой экономики. Литературный обзор выполнен с целью сбора данных об исследовании информационной безопасности и получения более глубоких знаний об информационной безопасности. Другой подход, который был использован при сборе информации об информационной безопасности, заключается в рассмотрении отечественного и зарубежного контента статей на данную тематику.

**Основная часть.** В общем случае информационная безопасность может быть определена как защита данных, принадлежащих организации или физическому лицу, от угроз и рисков.

Согласно словарю «Merriam-Webster», безопасность в целом - это качество или состояние защищенности, то есть быть защищенным от вреда. Согласно Оксфордскому студенческому словарю «Advanced», в более широком смысле безопасность - это принимаемые меры по обеспечению безопасности страны, людей, ценных вещей и т.д. Цель обеспечения безопасности заключается в создании защиты от врагов, кто может причинить ущерб, преднамеренный или иной. [3]

Информационная безопасность — это совокупность технологий, стандартов, политик и методов управления, которые применяются к информации для обеспечения ее безопасности.

Информационная безопасность выполняет четыре важные функции для организации, которая обеспечивает безопасную эксплуатацию приложения, реализованного на информационных технологиях (ИТ) систем организации, защищает данные, которые собирают и используют организации, гарантирует технологические активы, используемые в организации и, наконец, защищает способность организации функционировать.

Информационная безопасность обеспечивает защиту данных, которые организация собирает и использует. Если информация остается незащищенной, то к ней может получить доступ любой желающий. Если информация попадает не в те руки, она может разрушить жизнь, отбросить бизнес, а также может быть использована для нанесения вреда. Программы информационной безопасности гарантируют, что соответствующая информация будет защищена как деловыми, так и юридическими требованиями путем принятия мер по защите данных организаций. Кроме того, принятые меры по защите информации организаций являются вопросом сохранения конфиденциальности и помогут предотвратить кражу личных данных. [7]

В организации информация является важным бизнес-активом и имеет важное значение для бизнеса и, следовательно, нуждается в соответствующей защите. Это особенно важно в условиях все более взаимосвязанной деловой среды, в которой информация в настоящее время подвергается все большему числу и все более широкому спектру угроз и уязвимостей. Нанесение ущерба, такого как вредоносный код, взлом компьютера и отказ в обслуживании стали более распространенными, амбициозными и сложными. Таким образом, реализовав информационную безопасность в организации, он может защитить технологические активы, используемые в организации. [1]

**Проблемы в области информационной безопасности.** В нашем постоянно меняющемся мире для коммерческих организаций в условиях цифровой экономики существует множество проблем, которые затрудняют адекватную защиту ресурсов:

1. Объединение корпоративной и личной жизни.

2. Неправильное непоследовательное применение политик информационной безопасности.

3. Недостаточная информированность в области информационной безопасности.

4. Внутренние и внешние угрозы информационной безопасности и т. д. [2]

***1.*** ***Объединение корпоративной и личной жизни***. Бесплатные интернет-услуги, которые сотрудник имеет в своей организации, он может использовать в личных целях. Например, сотрудники используют электронную почту компании для некоторых личных коммуникаций, а некоторым сотрудникам может быть выдан мобильный телефон, который они используют для ограниченного личного использования. Многие люди могут даже не иметь домашний компьютер и использовать ноутбук компании для всего, включая запуск личного программного обеспечения. В других случаях сотрудники могут принести персональный ноутбук в офис и попытаться подключить его к рабочей сети компании. Это позволяет сотрудникам использовать актив организации, который функционирует для доступа и хранения информации организации в личных целях. Риск этого действия заключается в том, что информация может быть доступна другим лицам из внешних организаций.

***2. Неправильное непоследовательное применение политик информационной безопасности***. Многие организации используют политику безопасности непоследовательно. Ведь, вопросы информационной безопасности нельзя начинать с середины, надо продумать каждый шаг, начиная с самого начала. Если нет своих специалистов, привлекать извне, посылать на повышение квалификации.

Это вызывает много проблем, когда функцию безопасности пытаются взломать нарушители. Многие предприятия недооценивают важность осуществления политики и регулирования в области информационной безопасности. Это заставляет многие организации писать информационные политики, но не применять их.

***3. Недостаточная осведомленность в вопросах информационной безопасности***. Отсутствие у сотрудников знания основ информационной безопасности ставят в тупик вопросы безопасности. Незнание увеличивает шансы злоумышленников реализовывать атаки и кражи информации. В основном, сотрудники защищают информацию, но они не принимают надлежащие методы в обеспечении её безопасности, что, в свою очередь, ставит под угрозу конфиденциальную информацию.

***4. Внутренние и внешние угрозы информационной безопасности***. Новые угрозы безопасности возникают каждый день от вредоносных программ, которые могут быть непреднамеренно установлены на компьютере пользователя, до фишинговых попыток, которые обманывают сотрудников в предоставлении конфиденциальной информации, вирусов, червей и стратегических попыток кражи личных данных. Иногда трудно справиться с угрозой, атакующей информацию в организациях. Во многом это связано с тем, что программы защиты, установленные в компьютерной системе для защиты данных, не являются функционирующими надлежащим образом или же они попросту недостаточно хороши.

Действительно, внутренние и внешние угрозы информационной безопасности становится тотальными, такие как взлом внешними игроками, кража конфиденциальной и частной информации внутренними сторонами, включая сотрудников, кибератаки, которые ищут уязвимые места и ведут к финансовым потерям.

Выше мы перечислили внешние и внутренние угрозы. Хотя хорошо известно, что внешние угрозы проявляются из-за хакеров и киберпреступников, использующих лазейки и уязвимости в ИТ-инфраструктуре, необходимо также отметить, что угрозы изнутри — это нечто такое же опасное, как и угрозы извне.

Действительно, в последние годы наблюдается растущая тенденция к тому, что киберпреступникам оказывают помощь внутренние субъекты внутри организаций, которые предоставляют им подробную внутреннюю информацию об организационных системах и ИТ-инфраструктуре.

Кроме того, было также обнаружено, что чаще всего именно инсайдеры позволяют хакерам извне проникать в организационные системы и создавать хаос.

С другой стороны, нельзя полностью игнорировать угрозы со стороны хакеров, которые пытаются проникнуть в ИТ-системы не только из скрытых побуждений, но и со стороны конкурентов и других субъектов, которые теперь вышли в киберпространство в качестве средства расширения своих конкурентных игр.

Более того, целые страны и их разведывательные службы в настоящее время занимаются кибер-взломами организаций своих соперничающих стран с целью нанесения им ущерба и экономических потерь. Это особенно важно в контексте соперничества между Соединенными Штатами, Китаем и Россией, в котором хакеры из всех стран, которым помогают и подстрекают их сторонники из коммерческих и национальных интересов безопасности, взламывают системы своих конкурентов, чтобы нанести ущерб и причинить экономические, финансовые и репутационные потери, помимо причинения сбоев в бизнесе. [3]

Таким образом, все эти аспекты означают, что профессионалы по безопасности в организациях должны обеспечить надежную защиту своих систем от этих многочисленных угроз и гарантировать, что их ИТ-активы и аппаратное обеспечение, а также ИТ-инфраструктура защищены. Действительно, с таким большим количеством угроз, скрывающихся в киберпространстве, нет ничего необычного в том, что организации возводят брандмауэры и ограничивают доступ к своим системам из внешних источников.

Это также является причиной того, что многие организации в последние годы предприняли шаги, которые ограничили бы использование интернета их сотрудниками, чтобы они не оставляли «цифровые следы» в киберпространстве, которые могут быть использованы злонамеренными хакерами и киберпреступниками.

Еще одной областью, вызывающей озабоченность у специалистов ИС, является растущее число случаев фишинга и кражи личных данных, которые гораздо серьезнее, когда речь идет о счетах руководителей и старших должностных лиц помимо руководства в их организациях.

Хотя кража личных данных и фишинг могут привести к убыткам для любого лица и организаций, где это затрагивает старших сотрудников, это может серьезно навредить организационным целям, поскольку большинство этих сотрудников будут иметь строго засекреченную и конфиденциальную информацию, хранящуюся в их системах.

Именно по этой причине многие профессионалы по безопасности сегодня выступают за безопасные и защищенные системы для менеджеров и старших руководителей, которые отличаются и более «огорожены», чем те, которые используются рядовыми сотрудниками.

Действительно, с таким большим беспокойством по поводу этих аспектов, специалисты также гарантируют, что выше определенного уровня в организациях, доступ к информационным технологиям и интернету осуществляется через выделенные и автономные линии, а не общий и общекорпоративный доступ, который имеют другие сотрудники.

Трудности в управлении информационной безопасностью обусловлены отсутствием должной квалификации в области информационной безопасности. Иногда организации не принимают всерьез вопрос о найме сотрудников на основе их квалификации. Это связано с тем, что есть организации, которые нанимают сотрудников для менеджера по информационной безопасности, но это не соответствует его квалификации или навыкам, которые он имеет в области информационной безопасности. Таким образом, это трудно для этого персонала, чтобы защитить данные организаций с надлежащей защитой. Это позволит другим злоумышленникам легче атаковать и украсть информацию, если сотрудники не имеют навыков или знаний о том, как защитить конфиденциальные данные.

**Рекомендации и методики по решению проблем информационной безопасности в коммерческих организациях:**

1. Не объединять корпоративную и личную жизнь. Сотрудники должны знать свои границы. Они должны уметь отличать свою личную жизнь от своей работы. Они не должны пользоваться преимуществами используемых компанией объектов для их личного пользования. Это важно для того, чтобы через него злоумышленники не смогли получить доступ к информационным потокам организации. Организация должна объяснить об этом персоналу, чтобы сотрудники знали, что они могут и не могут. Должен быть проведен инструктаж по информационной безопасности перед работой в организации, необходимо составить дополнительный договор о неразглашении секретной информации и по использованию рабочих ресурсов.

2. Следовать правилам и придерживаться этих правил. Организация должна разработать, внедрить и поддерживать политику в области информационной безопасности. Это необходимо для того, чтобы сотрудники соблюдали правила доступа к информации. Политики информационной безопасности очень важны в организации, потому что политика информационной безопасности определяет требования к информационной безопасности. Таким образом, организация должна регулярно пересматривать политику в целях удовлетворения требований организационной безопасности.

3. Повышение уровня информированности сотрудников по вопросам информационной безопасности. В целях повышения уровня информированности сотрудников по вопросам безопасности организация должна предпринять ряд шагов для повышения уровня информированности и понимания сотрудниками важных аспектов информационной безопасности. Метод, который может быть использован организацией, заключается в том, чтобы дать образование своим сотрудникам в области защиты информации и ресурсов. Реализуя этот метод, сотрудники могут иметь лучшее представление об информационной безопасности, а также могут хорошо защитить информацию. Сотрудники должны понимать и принимать риски, связанные с использованием технологий и Интернета, в частности. Зная об угрозах, которые присутствуют, они могут научиться использовать технологии осторожно, а не слепо принимать необдуманные поспешные решения.

4. Установка соответствующих программ защиты и использование средств и методов защиты. Сотрудники и персонал организаций должны убедиться, что компьютерная сеть организации надежно настроена и активно противостоят против известных угроз. Профессиональное сетевое обслуживание также должно помочь организации поддерживать безопасную виртуальную среду путем анализа всех компьютерных ресурсов и определения плана профилактического обслуживания. Это включает в себя регулярную очистку ненужных или небезопасного программного обеспечения, применение исправлений безопасности, таких как небольшие части программного обеспечения, предназначенные для повышения безопасности компьютера, и выполнение обычных проверок для проверки на наличие вторжений со стороны недоброжелателей. Организация также может проверять права доступа и иметь возможность настроить автоматизированную процедуру, которая требует от сотрудников регулярно менять свои пароли для дальнейшей защиты информационных ресурсов организации. Кроме того, должна быть установлена обновленная и последняя защитная антивирусная программа, чтобы защитить компьютер от атак вирусов.

5. Наем квалифицированных сотрудников. Для надежной защиты и обеспечения сохранности конфиденциальной информации организация должна нанимать ИТ-специалистов и сотрудников, имеющих соответствующую квалификацию по информационной безопасности. Это необходимо для того, чтобы сотрудник знал, что делать в случае возникновения проблемы, а также для защиты данных. Кроме того, ИТ-эксперт или квалифицированный персонал лучше разбираются в вопросах информационной безопасности и знают, какие шаги необходимо предпринять для обеспечения сохранности информации. [2]

Вывод:

Информационная безопасность имеет решающее значение в организации. Вся информация, хранящаяся в организации, должна быть защищена. Информационная безопасность будет определяться как защита данных от любых вирусных угроз. Информационная безопасность важна в организации, потому что она может защитить конфиденциальную информацию, обеспечивает функционирование организации, а также обеспечивает безопасную работу приложений, реализованных в системе информационных технологий организации, и информация является важным ресурсом для организации. Даже если информация важна в организации, есть несколько проблем для защиты и управления информацией. Одной из проблем, с которыми сталкивается организация, является отсутствие понимания важности обеспечения информационной безопасности. Когда у сотрудников отсутствует знание информационной безопасности в плане хранения своей информации, организация легко подвергается атакам хакеров или другим угрозам, которые пытаются украсть или получить конфиденциальную информацию организации. Таким образом, для сотрудников организации крайне важно иметь знание и понимание о важности практики информационной безопасности в организации для защиты конфиденциальных данных.

**Список использованных источников:**

1. Информационное общество. [Электронный ресурс]// режим доступа: https://what-when-how.com/sociology/information-society/ (в свободном доступе)

2. Важность информационной безопасности в организациях. [Электронный ресурс]// режим доступа: https://www.uniassignment.com/essay-samples/information-technology/importance-of-information-security-in-organizations-information-technology-essay.php (в свободном доступе)

3. Угрозы информационной безопасности в организациях и обеспечение их предотвращения. [Электронный ресурс]// режим доступа: https://www.managementstudyguide.com/information-security-threats-and-prevention-and-recovery.htm (в свободном доступе)

4. Что такое цифровая экономика - описание термина. [Электронный ресурс]// режим доступа: https://prostocoin.com/finance/digital-economy (в свободном доступе)

5. Цифровая экономика. [Электронный ресурс]// режим доступа: https://en.wikipedia.org/wiki/Digital\_economy (в свободном доступе)

6. Почему информация нуждается в безопасности? [Электронный ресурс]// режим доступа: http://www.information-security-news.com/2014/01/25/information-security/ (в свободном доступе)

7. Что такое информационная безопасность? Почему это важно, перспективы работы и многое другое! [Электронный ресурс]// режим доступа: https://www.snhu.edu/about-us/newsroom/2018/06/what-is-information-security (в свободном доступе)