ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ОСНОВА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ КАЖДОГО ХОЗЯЙСТВУЮЩЕГО СУБЪЕКТА

[1]Ходжарахманова Назира Бахтияр кизи

[1]Магистр, Ташкентского государственного экономического университета

Аннотация

Статья содержит примеры нарушений информационной безопасности и их последствия, что помогает понять масштаб проблемы. Также приведены статистические данные о росте киберугроз и уязвимостей информационных систем. Для более глубокого анализа использовались методы индукции, дедукции и статистического анализа. Проведенный анализ позволяет выявить основные уязвимости и проблемы в области информационной безопасности, а также предложить потенциальные пути и стратегии их решения.

Ключевые слова: ❖ *Информационная безопасность, экономическая безопасность, хозяйствующие субъекты.*

Введение.

В современном мире информационная безопасность стала неотъемлемой частью стабильного развития любого хозяйствующего субъекта. С увеличением объемов ценных данных, хранимых в онлайн режиме, угрозы кибератак и киберпреступности стали более опасными. Нарушение информационной безопасности может привести к серьезным последствиям, включая утечку конфиденциальной информации, нарушение работы систем и даже финансовые потери. Для обеспечения полной безопасности и предотвращения потенциальных угроз необходимо активно работать над защитой информационных систем.

Информационная безопасность играет ключевую роль в обеспечении экономической безопасности государства и бизнеса. В современном мире, где информационные технологии проникают во все сферы жизни и деятельности, защита информации становится необходимостью для предотвращения угроз, связанных с кибератаками, кражей конфиденциальных данных, шпионажем и другими видами киберпреступности.

Экономическая безопасность страны зависит от сохранности ее информационных ресурсов. Киберугрозы могут привести к серьезным экономическим потерям, нарушению работы критической инфраструктуры, разрушению бизнес-процессов и довести до банкротства компании. Поэтому защита информации становится важным элементом обеспечения устойчивого развития экономики. Организации должны уделять особое внимание созданию и поддержанию системы информационной безопасности, которая включает в себя политику безопасности, технические меры защиты, обучение персонала, мониторинг и анализ угроз. Также необходимо учитывать законодательные требования по защите персональных данных и конфиденциальной информации.

Развитие кибербезопасности способствует укреплению доверия бизнес-партнеров, клиентов и инвесторов, что в свою очередь способствует росту экономики и привлечению инвестиций. Информационная безопасность становится ключевым фактором конкурентоспособности компаний на рынке. Таким образом, информационная безопасность является неотъемлемой частью экономической безопасности и требует постоянного внимания и инвестиций со стороны государства и бизнеса для обеспечения стабильности и устойчивости экономики.

Обзор литературы.

Значительный вклад в развитие концепции информационной безопасности внесли зарубежные ученые, такие как Брус Шнайер, который в своей книге “Secrets and Lies: Digital Security in a Networked World” подчеркивает важность защиты информации как ключевого элемента устойчивого функционирования бизнеса и государства. Шнайер рассматривает практические подходы к минимизации киберугроз и объясняет, как компании могут адаптировать свои стратегии безопасности в условиях динамично меняющегося технологического ландшафта [1].

Исследование Трента Джаггера "Managing Cybersecurity Risk" акцентирует внимание на управлении рисками в сфере кибербезопасности. Автор подчеркивает необходимость комплексного подхода, включая оценку рисков, технические меры защиты и разработку стратегий реагирования на инциденты [2].

Российский исследователь А.А. Орлов в своих иследованиях акцентирует внимание на экономических последствиях киберугроз. В книге “Экономическая безопасность в условиях цифровизации” анализирует влияние информационной безопасности на конкурентоспособность компаний и предлагает стратегические подходы к обеспечению устойчивости бизнеса [3].

И.С. Карпов в статье “Информационная безопасность и ее значение для бизнеса" рассматривает влияние утечек данных и кибератак на финансовую стабильность компаний. Автор предлагает методологию анализа уязвимостей информационных систем и оценивает их экономические последствия [4].

Среди узбекских авторов можно выделить Ш.Ю. Ибрагимова, который в статье "Информационная безопасность в условиях цифровой экономики Узбекистана” подчеркивает важность национальных стратегий по обеспечению защиты информационных систем. Автор также анализирует текущую правовую базу и ее влияние на устойчивость бизнеса [5].

Работа Д.Ж. Рахимова “Влияние киберугроз на экономическую безопасность Узбекистана” фокусируется на статистике киберугроз в регионе и подчеркивает необходимость повышения уровня осведомленности среди руководителей компаний о важности защиты информации [6].

Исследование Джеймса Эндрюса “Global Trends in Cybersecurity” предоставляет обширный анализ мировых тенденций в области информационной безопасности. Автор акцентирует внимание на международном сотрудничестве, необходимом для борьбы с глобальными киберугрозами, и предлагает модели для разработки национальных стратегий [7].

Анализ литературных источников показывает, что информационная безопасность является многоаспектной проблемой, требующей комплексного подхода, включающего технические, экономические и организационные меры. Зарубежные, российские и узбекские

исследования подчеркивают необходимость разработки эффективных стратегий для защиты информации, а также интеграции вопросов кибербезопасности в общую систему экономической безопасности.

Методология исследования.

Для исследования информационной безопасности хозяйствующих субъектов использовался комплексный подход, включающий анализ статистических данных, метод абстракции, системный анализ, а также методы индукции и дедукции. Анализ статистики позволил выявить масштабы и частоту киберугроз, а метод абстракции помог сосредоточиться на ключевых аспектах проблемы, таких как человеческий фактор и технические меры защиты. Системный подход обеспечил изучение взаимосвязей между организационными, техническими и поведенческими аспектами информационной безопасности, а статистический анализ выявил зависимости между действиями сотрудников и утечками данных. На основе полученных данных были разработаны практические рекомендации по минимизации рисков и повышению уровня защиты информации.

Анализ и результаты.

Информационная безопасность действительно играет ключевую роль в современном мире, где данные стали одним из самых ценных ресурсов. С развитием технологий и переходом к онлайн хранению данных, обеспечение безопасности информации стало более сложным и важным заданием для любого хозяйствующего субъекта. Раньше базы данных хранились в специальных архивах в распечатанном виде, что делало их уязвимыми для физического доступа и повреждений. Сейчас же они хранятся в онлайн виде, что обеспечивает огромные преимущества, такие как масштабируемость, быстрый доступ к данным, возможность резервного копирования и многие другие.

Однако переход к онлайн хранению данных также привел к увеличению угроз со стороны киберпреступников. Хакеры активно используют различные методы для взлома систем и кражи конфиденциальной информации. Это создает серьезные риски для компаний, организаций и государств, поскольку утечка данных может привести к финансовым потерям, нарушению репутации и даже угрозам национальной безопасности.

Информационная безопасность стала неотъемлемой частью экономической безопасности, поскольку она напрямую влияет на стабильность и надежность работы любого хозяйствующего субъекта. Многие ученые и специалисты по безопасности информации активно изучают эту проблему и разрабатывают новые методы защиты данных. В своих научных работах они предлагают различные подходы к определению понятия “информационная безопасность”, выделяя ключевые аспекты и принципы защиты информации.

В своей книге об информационной безопасности авторы Прожерин В.Г., Войтик А.И., утверждают, что информация как товар обладает уникальной спецификой, которая отличает ее от других товаров:

1) Она является предметом труда и средством труда, аналогично земле, но не обладает природными качествами.

2) Информация принимает форму продукта труда и услуги из-за широкого спектра отраслей, связанных с ее производством и использованием.

3) Лишь небольшая часть информации имеет товарную форму и стоимостную оценку.

4) Информация является объектом персонифицированной собственности, не отчуждается в актах купли-продажи.

5) Ценность информации определяется относительно цели, для которой она используется.

6) Информация полезна как для отдельного потребителя, так и для общества в целом.

7) Информацию можно использовать многократно без потери потребительских свойств.

8) Для фирмы информация является ключевым источником знаний о среде и продукции.

9) Для общества информация интеллектуализирует окружающую среду, создавая "инфосферу".

10) Информация представляет собой кодифицированное знание, требующее специфического подхода к передаче и использованию [8].

Таким образом, информационная безопасность является одним из самых важных аспектов современного мира, требующим постоянного внимания и развития. Обеспечение защиты данных становится все более сложным и требует комплексного подхода, включающего технические, организационные и человеческие меры. Ответственное отношение к информационной безопасности поможет предотвратить угрозы и обеспечить стабильное функционирование информационных систем в цифровой эпохе.

В своем учебном пособии С. И. Макаренко выделяет 3 основных составляющих информационной безопасности, таких как доступность, целостность и конфиденциальность.

Доступность информационных ресурсов означает возможность получения необходимой информации в разумные сроки.

Целостность информации подразумевает ее актуальность, непротиворечивость и защищенность от повреждений или несанкционированных изменений.

Конфиденциальность информации обеспечивает защиту от несанкционированного доступа к ней [9].

С развитием информационных технологий и распространением цифровых технологий в различных сферах деятельности, киберпреступности стали одной из наиболее актуальных проблем. Киберпреступники используют новейшие технологии для совершения различных преступлений, таких как кража конфиденциальных данных, финансовые мошенничества, кибершпионаж, кибертерроризм и другие виды атак.

Самыми распространенными способами совершения киберпреступлений являются фишинг (мошеннические попытки получить конфиденциальные данные через электронные сообщения), вредоносное программное обеспечение (вирусы, троянские программы и др.), DDoS-атаки (атаки на сервер с целью перегрузки его ресурсов), киберкражи (кража финансовых данных или личной информации) и другие.

Для эффективной борьбы с киберугрозами необходимо не только анализировать количество и виды киберпреступлений, но и обеспечивать финансирование в области кибербезопасности. Финансирование в этой сфере играет ключевую роль, поскольку позволяет развивать и совершенствовать технологии защиты, обучать специалистов, проводить исследования и анализ угроз.

Для полного анализа следует пользоваться статистическими данными и определить количество и способы совершения кибер преступностей. Для начало рассмотрим какие виды преступлений широко распространены и

насколько часто субъекты становятся жертвами. В последнее десятилетие угрозы информационной безопасности стали эволюционировать, переходя от прямых хакерских атак к методам социальной инженерии. Это связано с тем, что человек стал более уязвимой мишенью для киберпреступников, чем технические защиты. Утечки информации внутри компаний стали более распространенными из-за участия сотрудников в целенаправленных действиях.

Более 92,6% компаний сталкивались с утечками информации, причем в 55,2% случаев причиной были действия сотрудников. Они могут красть данные для различных целей, таких как продажа конкурентам или личное обогащение. Небрежное поведение персонала также является причиной утечек в 23,6% случаев.

Инсайдеры, действуя по-разному, могут привести к серьезным последствиям для компании. Например, в 61,5% случаев они могут привести к потере ценных коммерческих данных и новых разработок компании. Кроме того, сотрудники могут стать “кротами” (37%), продавцами информации (37%) или использовать ресурсы компании для своего личного бизнеса (26%).

Эти данные подчеркивают важность обучения персонала по вопросам информационной безопасности, контроля доступа к конфиденциальным данным и внедрения соответствующих политик и процедур для предотвращения утечек информации изнутри компании.

Рисунок 1. Доля участия работников в процессе утечки данных [15]

На сегодняшний день одним из основных видов угроз является внутренняя угроза, когда сотрудники компании имеют доступ к ценной информации и могут использовать её в своих корыстных целях.

С другой стороны, также имеются внешние риски. Отчет ENISA Threat Landscape (ETL) — это ежегодный отчет Агентства Европейского Союза по кибербезопасности ENISA о состоянии ландшафта угроз кибербезопасности. В октябре 2022 года ENISA опубликовало 10-е издание отчета, охватывающее период отчетности с апреля 2021 года по июль 2022 года. ENISA разделила основные угрозы на 8 групп. Частота и воздействие определяют, насколько заметны все эти угрозы.

• **Программы-вымогатели:** Это вредоносные программы, которые заражают компьютер и блокируют доступ к данным или устройству до тех пор, пока не будет выплачен выкуп. Они стали одной из самых серьезных угроз в последние годы, так как многие организации и частные лица сталкиваются с потерей доступа к своим данным. По данным, 60% пострадавших организаций могли платить выкуп.

• **Вредоносное ПО:** Это программное обеспечение, разработанное для нанесения ущерба компьютерам, сетям или данным. Раскрытия уязвимостей нулевого дня указывают на то, что злоумышленники активно ищут и используют новые способы атаки. В 2021 году наблюдалось 66 раскрытий уязвимостей нулевого дня (новый вид атак, используемый злоумышленниками).

• **Социальная инженерия:** Это метод манипуляции людьми с целью получения конфиденциальной информации. Фишинг - один из наиболее распространенных видов социальной инженерии, когда злоумышленники выдают себя за надежные организации, чтобы убедить людей предоставить им свои учетные данные. Фишинг остается популярным методом, но также появляются новые формы фишинга, такие как целевой фишинг, китобойный промысел, смишинг и вишинг.

• **Угрозы данным:** Это угрозы, связанные с конфиденциальностью, целостностью и доступностью данных. Увеличение количества полученных данных увеличивает риск их утраты или утечки. Увеличение пропорционально общему количеству полученных данных

• **Угрозы доступности:** Крупнейшая за всю историю атака типа «отказ в обслуживании» (DDoS) была запущена в Европе в июле 2022 года. Атаки типа DDoS направлены на перегрузку целевого ресурса, что приводит к недоступности для обычных пользователей. Крупномасштабные атаки DDoS могут существенно повлиять на работу организаций и сервисов.

• **Дезинформация:** Растущая дезинформация с использованием искусственного интеллекта и дипфейки. Это распространение ложной или вводящей в заблуждение информации с целью воздействия на общественное мнение или поведение. С использованием искусственного интеллекта и других технологий дезинформация становится более совершенной и труднее отличить от правдивой информации.

• **Целевая цепочка поставок:** На долю сторонних инцидентов приходится 17% вторжений в 2021 году по сравнению с менее чем 1% в 2020 году[1].

А что насчет затратов на обеспечения информационной безопасности?

Затраты на информационную безопасность неизбежны, однако их можно существенно уменьшить или исключить при правильной политике и профилактике нарушений. При соблюдении политики безопасности и предотвращении нарушений возможно исключить или существенно сократить следующие затраты:

- Восстановление системы безопасности до соответствия требованиям политики безопасности.
- Восстановление ресурсов информационной среды предприятия.
- Переделки внутри системы безопасности.
- Юридические споры и выплаты компенсаций.

[1]Отчет ENISA Threat Landscape (ETL) — это ежегодный отчет Агентства Европейского Союза по кибербезопасности ENISA о состоянии ландшафта угроз кибербезопасности.

URL: https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends

- Выявление причин нарушения политики безопасности.

Необходимые затраты включают в себя те расходы, которые необходимы даже при низком уровне угроз безопасности для поддержания достигнутого уровня защищенности информационной среды предприятия. Неизбежные затраты могут включать:

- Обслуживание технических средств защиты.

- Конфиденциальное делопроизводство.

- Функционирование и аудит системы безопасности.

Затраты на информационную безопасность напрямую влияют на уровень защищенности компьютерной информационной системы (КИС). Чем больше средств выделено на обеспечение безопасности, тем выше будет уровень защиты информационной среды предприятия. Общие затраты на безопасность включают в себя затраты на предупредительные мероприятия, контроль и восполнение потерь. При изменении уровня защищенности информационной среды меняются и величины этих затрат. Следовательно, сумма общих затрат на безопасность также изменяется.

Путем увеличения затрат на предупредительные мероприятия, связанные с обслуживанием системы защиты, можно повысить уровень защиты и снизить информационный риск. Это позволяет уменьшить затраты на компенсацию убытков от нарушений политики безопасности.

Таким образом, оптимальное распределение затрат на информационную безопасность позволяет достичь высокого уровня защиты информационной среды предприятия при минимальных потерях от возможных инцидентов.

Эффективные стратегии обеспечения информационной безопасности хозяйствующих субъектов

Комплекс мероприятий, направленных на устранение угроз информационной безопасности, должен быть целенаправленным и систематическим. Вот несколько ключевых шагов, которые могут быть включены в такой комплекс:

Рисунок 2. Комплекс мероприятий, направленных на устранение угроз информационной безопасности [15]

Обеспечение информационной безопасности является важной задачей для стабильного функционирования хозяйствующих субъектов. Для достижения высокого уровня защиты информации требуется комплексный подход, включающий разработку политик безопасности, обучение сотрудников, управление доступом и регулярное обновление программного обеспечения. Разработка и внедрение политик безопасности информации позволяет установить стандарты и правила работы с данными, а также определить порядок их защиты. Регулярные аудиты помогают оценить эффективность мер безопасности и своевременно выявить уязвимости. Как отмечает Е.В. Вострецова, формализация процессов управления безопасностью способствует минимизации рисков утечки информации [10]. В.Н. Ясенев подчеркивает, что такая систематизация помогает организациям оперативно адаптироваться к изменяющимся угрозам [11].

Особое внимание следует уделить обучению и повышению осведомленности сотрудников. Исследования показывают, что человеческий фактор является основной причиной утечек данных. Регулярные тренинги и образовательные программы позволяют снизить вероятность несанкционированного доступа и утечек информации. В.В. Андрианов и его соавторы отмечают, что такие меры укрепляют дисциплину и ответственность персонала [13]. Эффективное управление доступом играет ключевую роль в обеспечении информационной безопасности. Реализация принципа минимальных привилегий, при котором доступ к данным предоставляется только в объеме, необходимом для выполнения служебных обязанностей, значительно снижает вероятность внутренних угроз. Введение современных систем мониторинга и анализа инцидентов обеспечивает оперативное выявление угроз и их устранение [11]. Регулярное обновление программного обеспечения является важным элементом защиты. Вострецова Е.В. указывает, что своевременное устранение уязвимостей с помощью обновлений и патчей значительно снижает риски кибератак [10]. Кроме того, использование технологий шифрования данных и создание резервных копий помогают защитить конфиденциальную информацию и обеспечить восстановление данных в случае утраты или повреждения [13].

Международное сотрудничество также играет важную роль в повышении уровня информационной безопасности. В отчете ФАТФ подчеркивается, что объединение данных и совместный анализ позволяют более эффективно выявлять сложные угрозы, такие как киберпреступность и отмывание денег. Применение международных стандартов повышает доверие между участниками рынка и улучшает защиту данных [14].

Комплексное применение этих стратегий позволяет минимизировать риски утечек и обеспечить надежную защиту информации, что способствует устойчивому развитию хозяйствующих субъектов и укреплению их конкурентных позиций.

Заключение.

Информационная безопасность является неотъемлемой составляющей экономической безопасности каждого хозяйствующего субъекта в современном мире, где цифровые технологии играют ключевую роль во всех аспектах бизнеса. Защита информации от угроз и атак имеет решающее значение для сохранности финансовых и репутационных ресурсов компании, обеспечения непрерывности бизнес-процессов и защиты интересов клиентов и партнеров.

С учетом увеличения числа кибератак и усовершенствования методов атакующих, обеспечение информационной безопасности становится более сложной и важной задачей. При этом ключевым фактором успешной защиты является комплексный подход, включающий в себя разработку и внедрение политик безопасности информации, обучение и осведомленность сотрудников, управление доступом, шифрование данных, регулярное обновление программного обеспечения, создание резервных копий данных, мониторинг и обнаружение инцидентов, аудит безопасности и соблюдение законодательства.

Эффективная информационная безопасность обеспечивает не только защиту от угроз, но и способствует повышению доверия со стороны клиентов и инвесторов, улучшению репутации компании и обеспечению устойчивого развития бизнеса в цифровой среде. Поэтому каждый хозяйствующий субъект должен придавать информационной безопасности высший приоритет и интегрировать её в свою стратегию управления рисками и развития.

Список литературы.

1. Schneier, B. Secrets and Lies: Digital Security in a Networked World. Wiley, 2000. 432 с. С. 56–78.
2. Jagger, T. Managing Cybersecurity Risk. Springer, 2018. 284 с. С. 112–135.
3. Орлов А.А. Экономическая безопасность в условиях цифровизации. М.: Юрайт, 2021. 310 с. С. 145–162.
4. Карпов И.С. Информационная безопасность и ее значение для бизнеса // Вопросы экономики и права. 2022. № 4. С. 7–12.
5. Ибрагимов Ш.Ю. Информационная безопасность в условиях цифровой экономики Узбекистана // Экономика и управление. 2023. № 2. С. 3–9.
6. Рахимов Д.Ж. Влияние киберугроз на экономическую безопасность Узбекистана // Теория и практика экономики. 2022. № 1. С. 5–8.
7. Andrews, J. Global Trends in Cybersecurity. Oxford University Press, 2021. 365 с. С. 200–225.
8. А.И. Войтик, В.Г. Прожерин Экономика информационной безопасности: Учебное пособие. – СПб.: НИУ ИТМО, 2012. – 120 с. 6-7 стр.
9. Макаренко С. И. Информационная безопасность: учебное пособие. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.: ил 23 стр.
10.Основы информационной безопасности: учебное пособие для студентов вузов / Е.В. Вострецова.— Екатеринбург : Изд-во Урал. ун-та, 2019.— 204 с.
11. Ясенев В.Н. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЭКОНОМИЧЕСКИХ СИСТЕМАХ: Учебное пособие – Н. Новгород: Изд-во ННГУ, 2006 253 с
12. Информационная безопасность: экономические аспекты Информационная безопасность: экономические аспекты. ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 10 (125)/2003 Jet Info.
13. В. В. Андрианов С. Л. Зефиров В. Б. Голованов Н. А. Голдуев Обеспечение информационной безопасности бизнеса. 2010 г. 265 с.
14. ФАТФ (2021 г.) Критическая оценка объединения данных, совместного анализа и защиты данных, ФАТФ, Париж, Франция, https://www.fatf-gafi.org/publications/digitaltransformation/documents/data-pooling-collaborativeanalytics-data-protection.html
15. Исследование: угрозы информационной безопасности. Часть 1: статистика URL: https://stakhanovets.ru/blog/issledovanie-ugrozy-informacionnoj-bezopasnosti-chast-1-statistika/