УДК 004.04

ВЗАИМОСВЯЗЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

Немцева А. Д. студентка 1 курса СПУПСА факультета ПГС. Научный руководитель: Демьяненко Юлия Игоревна, ученая степень отсутствует, старший преподаватель. Сибирский государственный университет путей сообщения, г. Новосибирск

Информационные технологии — совокупность процессов, методов осуществления поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также пользования информацией и защиты информации Целью этого направления является получение новых знаний и создание информационных продуктов, отвечающих текущим потребностям людей.
В настоящее время информационные технологии активно используются в различных профессиональных сферах деятельности и заключаются в автоматизации трудового процесса, обработке и сортировке сведений.

Информационные технологии позволяют людям связываться друг с другом, находясь в отдаленных точках планеты, обеспечивают легкий доступ к данным и ресурсам. Это не только стимулирует технологический прогресс, но и открывает новые горизонты для совершенствования коммуникации людей [1] . ИТ-индустрия развивается быстрее других технологических отраслей, и регулярно появляются новые технологии. Это позволяет предприятиям и организациям находить нестандартные решения, оптимизировать процессы и повышать эффективность бизнеса. Автоматизируя задачи, вы можете уменьшить количество недочетов и увеличить результативность труда.

Сегодня информационные технологии обеспечивают сохранность конфиденциальных сведений и гарантируют безопасность. Это происходит в первую очередь благодаря криптографии.

Но с развитием ИТ-индустрии появились и угрозы, связанные с применением информационных технологий: растущее количество кибератак, вторжение злоумышленников в сети организаций, получение персональных сведений. Причиной этого являются: недостаточная осведомлённость населения, отсутствие квалификации и знаний о способах защиты от киберугроз, быстрое развитие технологий, развитие новых направлений, особенно в области искусственного интеллекта. Благодаря решениям на основе искусственного интеллекта автоматически выполняется поиск уязвимостей, анализ сведений для критически важных систем, что делает атаки более целенаправленными и масштабируемыми [2].

Обеспечение информационной безопасности - состояние защищенности информационных ресурсов (информационной среды) от внутренних и внешних

угроз, способных нанести ущерб интересам личности, общества, государства (национальным интересам).

Основная цель – это определение условий, которым должно подчиняться поведение системы, выработка критерия безопасности и проведение формального доказательства соответствия системы этому критерию при соблюдении установленных правил и ограничений. Виды угроз информационной безопасности описаны в таблице 1.

Таблица 1.

Тип угрозы	Описание	Пример
Угрозы конфиденциальности	Несанкционированный доступ к данным.	Получение посторонними лицами сведений о состоянии счетов клиентов банка.
Угрозы целостности	Несанкционированная модификация, дополнение или уничтожение данных.	Внесение изменений в бухгалтерские данные с целью хищения денежных средств.
Угрозы доступности	Ограничение или блокирование доступа к данным.	Невозможность подключиться к серверу с базой данных в результате DDoS-атаки.

В таблице 2 дана основная классификация информационных угроз и их описание.

Таблица 2

Классификация	**Тип угрозы**	**Описание**
По расположению источника	Внутренние	Источники угроз располагаются внутри информационной системы (например, недобросовестные сотрудники, ошибки в программном обеспечении).
	Внешние	Источники угроз находятся вне системы (например, хакерские атаки).
По размерам ущерба	Общие	Угрозы, нанесящие ущерб всему объекту безопасности в целом (например, полный отказ системы).
	Локальные	Угрозы, причиняющие вред отдельным частям объекта безопасности (например, нарушение работы конкретного сервиса).
	Частные	Угрозы, причиняющие вред отдельным свойствам элементов объекта безопасности (например, компрометация конкретных данных).

По степени воздействия	Пассивные	Угрозы, при которых структура и содержание информационной системы не изменяются (например, перехват данных без их изменения).
	Активные	Угрозы, при которых структура и содержание системы подвергается изменениям (например, внедрение вредоносного кода, модификация данных).
По природе возникновения	Естественные (объективные)	Угрозы, вызванные воздействием объективных физических процессов или стихийных природных явлений, не зависящих от воли человека (например, наводнение, землетрясение, сбой в электросети).
	Искусственные (субъективные)	Угрозы, вызванные воздействием на информационную сферу человека. (например, хакерские атаки, ошибки персонала).

Способы обеспечения информационной безопасности:

1. Используются методы шифрования информации для обеспечения конфиденциальности при хранении и передачи данных по сетям связи.
2. Осуществляется комплекс правил, которые регламентируют, какие пользователи или устройства имеют право работы с объектами или данными.
3. Используются программные решения или программно-аппаратные элементы компьютерных систем, которые обеспечивают защиту сегментов сети или отдельных хостов от неавторизированного доступа.
4. Внедряется антивирусная защита для профилактики и диагностики вирусного заражения, а также нежелательных программ и восстановления заражённых файлов.
5. Создание резервных копий данных на другом устройстве или в облачной инфраструктуре для быстрого восстановления в случае утери или повреждения носителя.
6. Использование DLP-систем, которые отслеживают все сообщения и документооборот, для предотвращения несанкционированного доступа к информации.
7. Проведение регулярных занятий с персоналом по информационной безопасности, осведомлённость сотрудников о рисках и методах защиты от киберугроз помогает поддерживать сохранность и безопасность данных.

Информационные технологии без обеспечения сохранности данных могут иметь уязвимости.

Отдел кадров организации собирает и хранит персональном информацию работающих сотрудниках, а специалисты по безопасности обеспечивают сохранность данной информации. Без тесного сотрудничества между этими группами не может быть обеспечена скоординированная работа по выявлению, устранению уязвимостей и наблюдению за процессами [3].

Специалисты по безопасности должны убедиться, что система учитывает актуальные требования к сохранению данных. Экспертам по кибербезопасности необходимо периодически проверять систему на наличие уязвимостей.

Отдел кадров также обязан обновлять программное обеспечение, чтобы улучшить параметры системы.

Целью информационных технологий является автоматизация бизнес-процессов, а также ускорение и упрощение многих процедур внутри компании [4]. Отдел информационных технологий отвечает за то, чтобы внедрение передовых информационных технологий не приводило к бизнес-рискам или утечке конфиденциальной информации [5].

Специалистам по персоналу важно разбираться в цифровых технологиях, выявлять потребности клиентов, а также планировать и организовывать рабочие процессы. Специалисты ИБ защищают данные от взлома, настраивают сети, ищут ошибки и недочеты, проводят сетевой анализ.

Поэтому сохранение данных должно быть приоритетом для всех, кто работает с ИТ-технологиями. Утечка или утрата конфиденциальных сведений может стать причиной ущерба репутации, денежных убытков и даже угрозы госбезопасности.

Библиографический список

1. Основы информационной безопасности: учебное пособие для студентов вузов / Е.В. Вострецова. — Екатеринбург: Изд-во Урал. ун-та, 2019.
2. Демьяненко Ю. И. Информационная образовательная среда подготовки специалистов инженерного профиля // Цифровые трансформации в образовании (E-Digital Siberia'2024): Материалы VIII Международной научно-практической конференции (Новосибирск, 2024 г.) Новосибирск: Изд-во СГУПС, 2024. С. 83–88.
3. Демьяненко Ю. И. Интеграция информационных технологий в образовательный процесс вуза // Информационные технологии и информационная безопасность в профессиональной деятельности: Материалы III Межвузовской научно-практической конференции с международным участием. (Новосибирск, 2024 г.) Новосибирск: Изд-во СГУПС, 2024. С. 36–40.
4. Демьяненко Ю. И. Информационно-коммуникационные технологии как средство формирования профессиональных компетенций учащихся. // Цифровые трансформации в образовании (E-Digital

Siberia'2021): Материалы V Международной научно-практической конференции (Новосибирск, 2021 г.) Новосибирск: Изд-во СГУПС, 2021. С. 73–77.

5. Информационные технологии в профессиональной деятельности [Электронный ресурс]: учеб. пособие / авт.-сост.: И. Ю. Куликова, Н. В. Муравьева, В. А. Боровых; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир: Изд-во ВлГУ, 2023.