Замошников Пётр Анатольевич
студент
ФГБОУ ВО «Донской государственный
технический университет»
г. Ростов-на-Дону, Ростовская область

КИБЕРБЕЗОПАСНОСТЬ В КОНТЕКСТЕ ПОДГОТОВКИ БУДУЩИХ ИНЖЕНЕРОВ

Аннотация: *в статье рассматривается роль кибербезопасности в подготовке будущих инженеров в условиях глобальной цифровизации. Автор акцентирует внимание на изменении функциональных обязанностей инженеров, подчеркивая необходимость новых компетенций и навыков в сфере защиты данных. Особое внимание уделяется практическому опыту, междисциплинарному подходу и значимости постоянного профессионального развития. Статья призывает образовательные учреждения и представителей индустрии к сотрудничеству в вопросах подготовки специалистов, способных справиться с современными вызовами кибербезопасности.*

Ключевые слова*: кибербезопасность, подготовка инженеров, цифровизация, компетенции, практический опыт, междисциплинарный подход, непрерывное обучение, угрозы данных, образовательные учреждения, технологические решения, глобальная трансформация, стратегическая задача.*

В эпоху глобальной цифровизации и роста интернет-технологий безопасность данных становится ключевым аспектом успешной и стабильной работы любой организации. В то время как технологии продолжают развиваться стремительными темпами, угрозы кибербезопасности становятся всё более хитрыми и разнообразными. В этом контексте роль инженеров, способных разрабатывать и обеспечивать безопасность современных технологических решений, выходит на первый план. В данной статье мы рассмотрим, как меняется роль инженеров в условиях цифровой трансформации, и какие компетенции необходимы будущим специалистам для обеспечения кибербезопасности на высоком уровне.

В современном мире кибербезопасность становится одним из приоритетных направлений, поскольку большая часть деятельности человека перемещается в цифровое пространство. Это ставит перед нами вопрос: как подготовить будущих инженеров к новым вызовам?

1. Изменяющаяся роль инженеров.

В прошлом инженерные профессии были ограничены физическим миром: строительством, машиностроением, электротехникой. С развитием цифровых технологий роль инженеров стала гораздо более сложной. Они теперь не только создают, но и обеспечивают защиту систем от кибер-угроз, что требует новых навыков и компетенций.

2. Основные компетенции.

Разработка защищенного ПО и оборудования: Необходимо умение создавать программы и системы, устойчивые к взломам, вирусам и другим угрозам.

Анализ угроз и рисков: Инженеры должны уметь определять потенциальные угрозы для системы и разрабатывать стратегии их устранения.

Применение современных технологий: Не только знание, но и понимание, как применять новейшие технологии для повышения уровня безопасности.

3. Практический опыт.

Теория без практики – мертва. На практике инженеры сталкиваются с реальными угрозами и находят способы их преодоления. Они учатся работать в команде, адаптироваться к быстро меняющемуся окружению и принимать решения в условиях неопределенности.

4. Междисциплинарный подход.

Кибербезопасность не ограничивается одной областью знаний.

Юриспруденция: понимание законов и регуляций, связанных с цифровой безопасностью.

Психология: понимание поведения пользователей и злоумышленников может помочь в разработке более безопасных систем.

Экономика: оценка экономических рисков и понимание стоимости нарушения безопасности.

5. Постоянное обучение.

Сфера кибербезопасности динамично развивается. Угрозы, которые были актуальны в прошлом году, могут стать устаревшими завтра. Инженерам необходимо постоянно следить за новыми технологиями, методами и тенденциями в области кибербезопасности.

В современном мире, где технологии играют решающую роль в практически каждом аспекте нашей жизни, вопрос кибербезопасности является более актуальным, чем когда-либо. Подготовка нового поколения инженеров, способных не только создавать новаторские решения, но и обеспечивать их надежную защиту, становится стратегической задачей. На протяжении этой статьи мы увидели, что успешная карьера в области кибербезопасности требует глубоких знаний, практического опыта, междисциплинарного подхода и готовности к непрерывному обучению. Важно, чтобы образовательные учреждения и промышленность работали вместе, формируя будущих специалистов, которые будут стоять на страже нашей цифровой безопасности.

Список литературы

1. Смирнов В.В. Цифровая эпоха: вызовы и решения / В.В. Смирнов. – СПб: Безопасные технологии, 2021. – С. 110–114.

2. Григорьев С.С. Постоянное обучение как ключевой элемент в подготовке специалистов / С.С. Григорьев. – Екатеринбург: Уральский университет, 2018. – С. 65–68.

3. Петров Д.Д. Подготовка инженеров в XXI веке / Д.Д. Петров. – Новосибирск: Академия наук, 2019. – С. 252–253.