Выводы

Проведенное исследование позволяет сделать вывод о том, что сетевые информационные технологии обладают значительным потенциалом для формирования познавательной самостоятельности старшеклассников. Однако их эффективность во многом зависит от педагогических условий, включающих в себя выбор качественных образовательных платформ, организацию интерактивного взаимодействия и персонализацию обучения.

Список литературы

1. Bukreiev D. et al. Features of the development of an automated educational and control complex for checking the quality of students. CEUR Workshop Proceedings, 2021.

2. Kruglyk V.S. et al. Using the Discord platform in the educational process // Proceedings of the symposium on advances in educational technology, aet. 2020.

3. Букреев Д.А., Барановская В.С. Персонализация интерактивных цифровых медиа в образовательной среде // Международный студенческий научный вестник. 2023. № 2.

4. Касьяненко М.М., Букреев Д.О. Анализ современных технологий электронного обучения // Информационные технологии в образовании и науке: сборник научных трудов II Международной научно-практической конференции. Мелитополь: ФЛП Однорог ТВ. 2021. С. 59-62.

О ПРОБЛЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Сафонова А.О., Сафонова П.О.

АНОО ВО «Воронежский институт высоких технологий», Воронеж, e-mail: bbosly@yandex.ru

Что касается данных компьютерной системы, то существует риск, связанный с их потерей из-за неисправности или разрушения компонентов оборудования [1].

Существует также риск кражи. Подходы к обеспечению информационной безопасности включают использование аппаратных средств и устройств. Также существует развертывание соответствующих аппаратных и программных компонентов.

Успешная борьба с фактом несанкционированного доступа к информации и процессами перехвата данных может основываться на четком представлении о том, какие каналы существуют для утечки информационных компонентов.

В интегральных схемах происходят высокочастотные изменения уровней напряжения и тока, на основе которых ведется наблюдение за работой компьютера. Вибрация распространяется по проводному соединению. В этом случае может произойти преобразование в понятную форму. Кроме того, существует возможность перехвата с помощью специальных устройств. Устройство может быть встроено в компьютер или монитор для перехвата информации [2]. Она будет выводиться на монитор или вводиться с клавиатуры. Существует вероятность перехвата при передаче информации по внешнему каналу связи. Это может быть телефонная линия.

На практике используется несколько наборов методов защиты [3]:

- препятствия, которые встают на пути похитителей, которые создаются с помощью физических и программных средств;

- это окажет воздействие на элементы управляемой или защищенной системы;

- выполнять преобразование данных, как правило, методами маскировки или шифрования;

- внедрение нормативных актов или разработка нормативных правовых актов, а также комплекса мер, направленных на стимулирование пользователей к взаимодействию с базой данных для совершения необходимых действий;

- принуждение, или создание таких условий, при которых пользователь вынужден соблюдать правила обработки данных;

- Мотивация, или формирование условий, которые побуждают пользователя к необходимым действиям.

Каждый метод защиты информации [4] реализуется на основе различных категорий инструментов. Основными инструментами являются организационные и технические.

Разработка комплекса организационных инструментов, связанных с защитой информации, должна рассматриваться в рамках компетенции служб безопасности.

Во многих случаях специалисты по безопасности [5]:

- разрабатывают внутренние документы, в которых указаны правила работы с элементами компьютерного оборудования и разделами конфиденциальной информации;

- подписывают дополнительный контракт к трудовому договору, в котором оговаривается ответственность за разглашение или неправомерное использование информации, ставшей известной на работе;

- разграничивают зону ответственности, чтобы исключить ситуации, при которых массив наиболее важных данных будет находиться в распоряжении одного из специалистов;

- внедряют программные продукты, защищающие данные от копирования и уничтожения пользователями, но это касается и топ-менеджеров компании;

- разрабатывают план восстановления системы в случае сбоя по любой причине.

Если в организации нет специализированной службы информационной безопасности, решение заключается в привлечении специалистов по безопасности на аутсорсинг. С помощью удаленных сотрудников проводится аудит ИТ-инфраструктуры компании и составляются рекомендации по защите от внешних и внутренних угроз. Даже при аутсорсинге предполагает-

ся, что для защиты корпоративной информации будут использоваться специальные программы.

Список литературы

1. Львович Я.Е., Преображенский А.П., Преображенский Ю.П., Клименко Ю.А. Анализ программно-технических решений блокировки запрещенной информации в информационно-телекоммуникационных сетях // Информационные технологии. 2022. Т. 28. № 8. С. 429-437.

2. Бормотов В.Е. Проблемы защиты информации в компьютерной сети // Молодой ученый. 2016. № 11 (115). С. 148-150. URL: https://moluch.ru/archive/115/31145/ (дата обращения: 15.01.2025).

3. Аветисян Т.В., Львович Я.Е., Преображенский А.П. Алгоритмы моделирования для оценки рисков в киберфизических системах // Телекоммуникации. 2023. № 2. С. 9-15.

4. Поначугин А.В. Проблемы и реализация комплекса мер безопасности компьютерных сетей // Вестник НГИЭИ. 2016. № 2 (57). URL: https://cyberleninka.ru/article/n/problemy-i-realizatsiya-kompleksa-mer-bezopasnosti-kompyuternyh-setey (дата обращения: 15.01.2025).

5. Келдыш Наталья Всеволодовна Системная защита информации компьютерных сетей: учебное пособие. М.: Мир науки, 2022. URL: https://izdmn.com/PDF/43MNNPU22.pdf (дата обращения: 15.01.2025).

БЕЗОПАСНАЯ РАЗРАБОТКА ВЕБ-ПРИЛОЖЕНИЯ ОБЪЕКТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ НА ОСНОВЕ ИНТЕГРАЦИИ МЕТОДОЛОГИИ DEVSECOPS В ПРОЦЕСС ПРОЕКТИРОВАНИЯ

Сверчков Р.В., Андрияхов Я.В.

Российский экономический университет им. Г. В. Плеханова, Москва, e-mail: rvsverchkov@gmail.com

Научный руководитель: Микрюков А.А.

Введение

В современных реалиях веб-приложения становятся все более сложными по технической реализации, что приводит к повышенной вероятности возникновения уязвимостей [5]. Вместе с этим возрастает и зависимость критической информационной инфраструктуры (КИИ) от применяемых решений и подходов к проектированию, что делает задачи по обеспечению киберустойчивости первостепенными [2].

Распространенные методы защиты (антивирусы, межсетевые экраны и т.д.) могут противостоять многим атакам, однако практика показывает, что при разработке программных продуктов вопросы информационной безопасности чаще всего рассматриваются лишь на заключительных этапах жизненного цикла. Это приводит к неэффективному выявлению и устранению уязвимостей и, как следствие, к большим затратам на их исправление [4]. С учетом этого использование интегрированных подходов на основе DevSecOps становится востребованным, особенно в сфере КИИ [3].

В данной статье предлагается усовершенствованный поэтапный подход к интеграции методологии DevSecOps, дополняющий стандартную схему встроенными механизмами количественной оценки уязвимостей и анализом затрат на их устранение. Также приводится сравнительная оценка предлагаемого решения с традиционными методами безопасной разработки, где меры защиты внедряются преимущественно на поздних стадиях SDLC (Systems development life cycle).

Целью данной работы является применение комплексного решения DevSecOps, адаптированного под задачи объектов КИИ, снижающего общее число уязвимостей и повышающего оперативность реагирования на угрозы.

Пример поэтапной интеграции DevSecOps при разработке веб-приложения для объекта критической информационной инфраструктуры

Создание современных веб-приложений требует особенного внимания к безопасности компонентов на каждом этапе жизненного цикла разработки [1]. Непосредственная интеграция мер защиты с учетом особенностей разработки веб-приложений позволяет значительно снизить риски, а также обеспечить надежную работу веб-приложений в условиях постоянно меняющихся киберугроз. Ниже приведен пример поэтапной интеграции DevSecOps в рамках разработки веб-приложения для системы управления водоснабжением города. Рассматриваемое приложение является объектом критической информационной инфраструктуры [2].

1. Планирование и анализ угроз;

Данный этап являются ключевыми в обеспечении информационной безопасности на ранних стадиях разработки. На этом этапе формируется перечень нормативных требований с учётом отечественных и международных стандартов (ФСТЭК, ГОСТ Р ИСО/МЭК 27001-2019, ISO/IEC 27001), проводится моделирование угроз по методологии STRIDE и определяются метрики, позволяющие объективно оценить уровень защищённости системы. Такой комплексный подход даёт возможность чётко обозначить приоритеты и сроки устранения уязвимостей, что существенно повышает надёжность и устойчивость будущего продукта к киберугрозам, а именно:

• Требования безопасности. Формируется перечень нормативных требований на основе стандартов ФСТЭК, ГОСТ Р ИСО/МЭК 27001-2019 [1], а также международных рекомендаций (ISO/IEC 27001);

• Моделирование угроз. Проводится сессия с применением методологии STRIDE [6], формируются сценарии возможных атак;

• Определение метрик. На этом этапе задаются целевые показатели: допустимое количе-