

Практическое занятие № 3

Тема: Современные методы обнаружения и нейтрализации угроз с помощью кроссплатформенных информационных систем. Примеры задач информационной безопасности и защиты данных средствами кроссплатформенного программирования.

Литература:

1. Импортозамещающие технологии обеспечения информационной безопасности и защиты данных (под ред. Л.В. Черкесовой). Ростов-на-Дону, 2020.
2. Квантовые вычислительные системы информационной безопасности: основы алгоритмического, программного и аппаратного обеспечения (под ред. Л.В. Черкесовой). Ростов-на-Дону, 2021.
3. Применение технологий искусственного интеллекта и поддержки принятия решений в задачах информационной безопасности (под ред. Л.В. Черкесовой). Ростов-на-Дону, 2022.
4. Биометрические средства идентификации и аутентификации человеческой личности в системах информационной безопасности (под ред. Л.В. Черкесовой). Ростов-на-Дону, 2024.

Вопросы:

1. Назовите методы, характеристики и области применения *биометрической идентификации и аутентификации* личности человека в программных средствах, применяемых в информационной безопасности и защиты данных. Приведите примеры.
2. Перечислите основные *статические* биометрические технологии распознавания личности человека – по отпечаткам пальцев, рисунку вен руки, радужной оболочке глаза, сетчатке глаза, рисунку вен лица, 2D–изображению лица, 3D–модели лица и др.
3. Расскажите об основных *динамических* биометрических технологиях идентификации/аутентификации личности человека – по почерку, голосу и устной речи, клавиатурному почерку, манере движения, движению губ, вибрации пальцев и др.
4. Какие биометрические технологии планируется использовать в ближайшем будущем? Как можно реализовать их с помощью *нейросетевых технологий*?
5. Назовите угрозы безопасности работы кроссплатформенных информационных систем, которые может представлять появление *квантовых компьютеров*?
6. Перечислите известные сегодня *квантовые алгоритмы* и их применение в задачах информационной безопасности. В чём состоит их потенциальная опасность (на примере квантового алгоритма факторизации и дискретного логарифмирования П. Шора)?
7. Что представляет собой *квантовая криптография* как область исследований? Перечислите основные протоколы квантового распределения ключей.
8. Расскажите о *квантовом хакинге* как о возможности взлома квантовых линий связи. В чём состоит уязвимость квантовых протоколов на практике?
9. Расскажите о возможности распознавания *деструктивных эмоций* человека по его изображению на фотографии или в видеопотоке. Можно ли распознать потенциального террориста до того момента, как он совершил террористический акт?
10. Как, с помощью нейросетевых технологий, можно распознать *деструктивные черты характера* человека по его рукописному почерку? Можно ли вычислить потенциального преступника, хакера, террориста, экстремиста, маньяка–убийцу?
11. Расскажите о возможности поиска *потенциально опасных конструкций* и уязвимостей в исходных текстах программ с помощью нейросетевых технологий.
12. Объясните работу информационной системы безопасности, предназначенной для *беспилотных транспортных средств* (на примере автомобильного транспорта).
13. Самостоятельное изучение самой свежей научной литературы (научных статей, монографий, учебников 2021 – 2024 годов издания) по теме занятия.