Информационная безопасность автоматизированных систем

Квалификация – техник по защите информации

Код специальности: **10.02.03**

Уровень образования: *специалист*

Актуальность обучения

В век информационных технологий главной ценностью становится информация. Достоверность и доступность являются важными её критериями. Поэтому так важно заботиться о её конфиденциальности и защите.

На сегодняшний день автоматизированные системы (АС) играют ключевую роль в обеспечении эффективного выполнения бизнес-процессов как коммерческих, так и государственных предприятий. Вместе с тем повсеместное использование АС для хранения, обработки и передачи информации приводит к повышению актуальности проблем, связанных с их защитой. Подтверждением этому служит тот факт, что **за последние несколько лет, как в России, так и в ведущих зарубежных странах имеет место тенденция увеличения числа информационных атак.**

Уязвимости - ахиллесова пята автоматизированных систем.

Практически любая автоматизированная система может выступать в качестве объекта информационной атаки – совокупности действий злоумышленника, направленных на нарушение одного из трёх свойств информации - **конфиденциальности, целостности или доступности.**

Примерами уязвимостей автоматизированных систем могут являться:

- некорректная конфигурация сетевых служб АС,
- наличие ПО без установленных модулей обновления,
- использование нестойких к угадыванию паролей,
- отсутствие необходимых средств защиты информации и др.

Уязвимости являются основной причиной возникновения информационных атак. Наличие слабых мест в автоматизированных системах может быть обусловлено самыми различными факторами, начиная с простой халатности сотрудников, и, заканчивая преднамеренными действиями злоумышленников.

Последствия, к которым могут привести информационные атаки, могут быть совершенно разного масштаба. Так, например, од но и тоже последствие атаки может сводиться к искажению системного файла на сервере для системного

администратора, в то время как для руководителя компании - приостановкой одного из важнейших бизнес-процессов предприятия.

В настоящее время успешная работа предприятий, использующих те или иные информационные системы, зависит от того насколько хорошо они защищены от возможных угроз безопасности. Это позволяет утверждать, что **проблема защиты информации является сегодня одной из наиболее злободневных и актуальных.**

Личные качества специалиста по защите информации

Создание и наладка информационных систем – это всегда работа нескольких специалистов: руководителя компании, аналитика, проектировщиков систем, программистов. Ко всем нужно найти подход и суметь поставить задачу понятным для них языком. А потому коммуникабельность и умение работать в команде для такого специалиста крайне необходимы.

Аналитический склад ума и умение планировать свою деятельность позволят специалисту проводить сложнейшие операции, разрабатывать компьютерные программы, работать с вычислительной техникой, быстро осваивать постоянно развивающийся рынок технологий. Хладнокровность и самообладание также пригодятся: в случае выхода из строя оборудования он должен приступить к устранению проблем, не подвергаясь панике. Также будут полезны хорошая память, внимательность и скрупулезность.

Работа с информацией - всегда ответственный труд. Поэтому от специалиста в сфере информатики и вычислительной техники требуется внимательность, оперативность, организованность и стрессоустойчивость.