**Вариативная самостоятельная работа № 6.**

1. Постановка задачи

6.1. Сформулируйте ваши предложения по нормализации работы с информационными технологиями и создания условий, в которых нарушать правила и законы было бы не выгодно.

Сформулируйте ваши предложения по повышению ответственности спец ИТ: как на них воздействовать.

Результат выполнения задания оформите в виде текстового файла. Опубликуйте в Moodle.

Результаты выполненной работы

Подключение без защиты

1. Весьма опасны подключения к внешним сетям через модемы минуя средства защиты (Firewall и другие общие меры безопасности). Тем самым создаются предпосылки для проникновения злоумышленников в корпоративную компьютерную сеть Компании.

Памятка: Прежде чем подключиться к внешним сетям обратитесь к специалисту по защите информации для решения всех вопросов по защите информационных ресурсов Компании

2. Сокрытие фактов нарушения информационной безопасности

Вы можете плохо знать общую политику информационной безопасности, но важно четко знать, что можно, а что нельзя.

Вы обязаны незамедлительно сообщать своему руководителю обо всех фактах нарушения политики информационной безопасности, которые стали вам известны.

Памятка: Помните, что успех компании (и ваша работа также) зависят от быстроты действий по предотвращению инцидентов безопасности. Требуйте от сотрудников незамедлительно сообщать такие факты при их выявлении.

3. Запоздалая реакция на изменение среды

В общем и прикладном программном обеспечении регулярно обнаруживаются уязвимости, способные привести к инцидентам безопасности.

Памятка: Важно не откладывать соответствующие модернизации программного обеспечения на потом, поскольку это может нанести Компании серьезные убытки.

4. Личная ответственность сотрудников

Большинство инцидентов безопасности (до 80%) возникают из-за действий собственных сотрудников компании, ее партнеров и подрядчиков.

Памятка: следует помнить, что любая информация, попавшая в чужие руки, может быть использована не по назначению и способна нанести ущерб ее репутации. Все члены нашего коллектива, а также наши партнеры, должны понять важность обеспечения безопасности при обращении с информацией, которая им доверена.

5. Подключение к сети предприятия посторонних носителей информации

Большинство инцидентов безопасности возникают из-за необдуманных действий собственных сотрудников Компании. Категорически запрещается приносить на рабочее место и работать на компьютерах, включенных в сеть Компании, любые личные накопители информации (диски, флэшки и подобное).

Памятка: все члены нашего коллектива, а также наши партнеры, должны обеспечить защиту от вредоносного ПО. Пользуйтесь исключительно носителями принадлежащими Компании и прошедшими проверку на безопасность.

6. Использование нелицензионного ПО

Часто предприниматели экономят на лицензионном ПО и работают на пиратском. Закон принят давно и с каждым днем шансы на его активизацию нарастают. Этим может и воспользоваться недобросовестные конкуренты.

Памятка: следует знать, что сегодня разработаны множество способов получения прав владения и использования ПО на легальной основе и за разумные деньги.