**Отчёт**

**Практическая работа Тестирование безопасности**

**Задание 1**. Проанализируйте данные нарушения:

**1. Сотрудники сидят в интернете на развлекательных сайтах по 4 часа.**

1) Грозит потерей времени и продуктивности работы, что может привести к снижению доходов компании и снижению конкурентоспособности.

2) Необходимо установить правила и нормы поведения в интернете, запрещающие доступ к развлекательным сайтам в рабочее время;

3) Сотрудников необходимо обучить правилам использования интернета в рабочее время.

**2. Играют в игры на работе.**

1) Общее падение производительности и продуктивности;

2) Сотрудники могут ввести компанию в неприемлемые риски за счет утечек программного обеспечения, которое может использоваться злоумышленниками для атак на внутренние сети;

3) Обоснованное использование системы мониторинга сотрудников за их работой.

**3. Перекладывают свои обязанности на других.**

1) Снижение эффективности работы для всей команды;

2) Может привести к ошибкам, несвоевременному исполнению обязанностей и пропуску задач;

3) Необходимо проводить тренинги для улучшения командного взаимодействия и распределения ролей внутри команды.

**4. Сотрудники копируют конфиденциальные данные компании.**

1) Утечка конфиденциальных данных может привести к репутационным и финансовым потерям компании;

2) Следует запретить перенос информации на внешние носители, установить контроль доступа и мониторинг операций, связанных с конфиденциальными данными;

3) Необходимо обучить сотрудников правилам обращения с конфиденциальной информацией.

**5. Сотрудники одновременно работают на другой работе.**

1) Грозит снижение производительности при основной работе и уменьшение эффективности работы на обеих работах;

2) Следует запретить работу на другой работе во время работы в компании и проводить мониторинг правильности использования времени на работе;

3) Необходимо обучить сотрудников правилам использования рабочего времени.

**6. Сотрудники работают на конкурента.**

1) Может привести к сокращению клиентской базы и убыткам компании;

2) Следует устанавливать контроль над информацией, в которой работают сотрудники, и мониторить их деятельность;

3) Нужно обучать сотрудников этикету профессиональной деятельности.

**7. Сотрудник хочет создать собственную конкурентную компанию.**

1) Утечка конфиденциальной информации и отток кадров;

2) Следует проводить тренинги и мониторинг деятельности сотрудников;

3) Необходимо позаботиться о социально-экономической защите и мотивации сотрудников.

**8. Сотрудники распространяют государственную тайну.**

1) Грозит уголовная ответственность для компании и сотрудников;

2) Необходимы меры по ужесточению мер контроля и мониторинга использования государственной тайны;

3) Нужно обучать сотрудников правилам работы с государственной тайной.

**9. Используется потенциально опасное ПО, содержащее уязвимости, позволяющие скрытую передачу данных, дающие возможность деструктивного влияния на ИТ инфраструктуру компании.**

1) Утечка конфиденциальных данных компании;

2) Следует убедиться, что ПО находится в адекватном состоянии, и обеспечивать обновление системы безопасности;

3) Необходимо обучать сотрудников проведению проверки и обнаружению потенциально опасных ПО.

**10. Выясняется, что административные пароли передаются по открытым каналам. Сотрудники используют средства удаленного управления.**

1) Грозит утечка конфиденциальных данных и нарушение целостности ИТ инфраструктуры компании;

2) Следует настроить удаленное управление компьютером для потенциально уязвимых компонентов системы;

3) Необходимо обучить сотрудников правилам использования административных паролей и мерам безопасности компании при работе с удаленным управлением.

**11. Администраторы сделали бреши в межсетевом периметре компании для удобства.**

1) Грозит нарушение целостности ИТ инфраструктуры, включая соответствующие законодательные нормы;

2) Следует настроить фильтрацию входящего и исходящего трафика для потенциально уязвимых компонентов системы;

3) Необходимо обучить администраторов мерам безопасности и настроить рутину проведения проверок.

**12. Оставлены закладки в самописном программном обеспечении.**

1) Грозит утечкой конфиденциальных данных компании;

2) Следует проверить наличие закладок и удалить их, если они найдены;

3) Необходимо обучить сотрудников правилам разработки и тестирования программного обеспечения.

**Задание 2:** Заполните таблицу

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № | Объект защиты | Наименование угрозы | Источник угрозы | Последствия | Как избежать угрозы |
| 1 | Банковская карта | 1. Смс мошенничество 2. Мошенничество через e-mail 3. Мошенничество через телефонные звонки 4. Мошенничество при заказе товаров и услуг через интернет-магазин 5. Мошенничество при расчётах пластиковой картой в магазине 6. Установка нелегальных считывающих устройств на банкоматах и использование нелегальных мобильных считывающих устройств 7. Потеря карты | Мошенники | Потеря доступа к карте и потеря денежных средств. | Требуйте проведения операций с Вашей картой только в Вашем присутствии, не позволяйте уносить карту из поля Вашего зрения. |
| 2 | Рабочее место директора | 1) Вредоносная рассылка  2) Использование непроверенных мессенджеров | Сам директор,  мошенники | Потеря конфиденциальной  информации | Директору стоит ознакомиться с безопасностью в интернете,  Использовать проверенные мессенджеры. |
| 3 | Домашний компьютер | 1. Редкое обновление антивирусных баз 2. Несанкционированное отключение элементов защиты пользователя 3. Использование сомнительного ПО 4. Отсутствие разграничения доступа 5. Разглашение конфиденциальной информации 6. Потеря носителей конфиденциальной информации 7. Вирусы | Мошенники, хакеры, пользователь | Потеря личных данных пользователя | Использование лицензионных программ, использование актуальной версии антивируса |
| 4 | Рабочее место в больнице | 1. Редкое обновление антивирусных баз 2. Несанкционированное отключение элементов защиты пользователя 3. Использование сомнительного ПО 4. Отсутствие разграничения доступа 5. Разглашение конфиденциальной информации 6. Потеря носителей конфиденциальной информации 7. Использование сотрудниками личной почты, социальных сетей и мессенджера | Вредоносные программы, хакеры, сотрудники | Утеря данных о клиентах больницы и их персональных данных | Использование лицензионных программ, использование актуальной версии антивируса, ограничить доступ сотрудникам в интернет, запретить вход в почту и соцсети. |
| 5 | Фирма по разработке ПО | 1. Редкое обновление антивирусных баз 2. **кража конфиденциальной информации путем взлома информационной системы** 3. **кража инсайдерами коммерческой тайны** 4. **вирусные заражения** 5. вредоносное ПО 6. хакерские атаки 7. Устаревшие или незрелые системы управления доступом | Вредоносные программы, хакеры, сотрудники | Потеря конфиденциальной информации | Использование лицензионных программ, использование актуальной версии. |
| 6 | Банкомат | 1. Malformed устройство 2. User Input Emulation 3. Троянские программы 4. Повышение привилегий 5. Подмена процессингового процессора 6. Вскрытие банкомата | Мошенники, хакеры | Утеря денежных средств | Размещать сетевое оборудование в пределах сервисной зоны банкомата.  Использовать программный или аппаратный VPN-клиент, размещаемый в сервисной зоне банкомата. |