**Практическая работа Тестирование безопасности**

**Задание 1**. Проанализируйте данные нарушения:

1. Сотрудники сидят в интернете на развлекательных сайтах по 4 часа.
2. Играют в игры на работе.
3. Перекладывают свои обязанности на других.
4. Сотрудники копируют конфиденциальные данные компании.
5. Сотрудники одновременно работают на другой работе.
6. Сотрудники работают на конкурента.
7. Сотрудник хочет создать собственную конкурентную компанию.
8. Сотрудники распространяют государственную тайну.
9. Используется потенциальное опасное ПО, содержащее уязвимости, позволяющие скрытую передачу данных, дающие возможность деструктивного влияния на ИТ инфраструктуру компании.
10. Выясняется, что административные пароли передаются по открытым каналам. Сотрудники используют средства удаленного управления.
11. Администраторы сделали бреши в межсетевом периметре компании для удобства.
12. Оставлены закладки в самописном программном обеспечении.

**Задание 2.** Ответьте на вопросы для каждого случая:

1. Чем могут грозить данные нарушения компании?

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

Потеря продуктивности, снижение качества работы, отвлечение внимания от основной задачи.

* Играют в игры на работе.

Потеря времени на выполнение основных задач, снижение производительности, отвлечение внимания.

* Перекладывают свои обязанности на других.

Повышенная нагрузка на коллег, ухудшение качества работы, недосып и перегрузка.

* Сотрудники копируют конфиденциальные данные компании.

Утечка конфиденциальной информации, нарушение законов о защите данных, угроза репутации компании.

* Сотрудники одновременно работают на другой работе.

Конфликт интересов, возможное использование корпоративных ресурсов для личных целей, снижение мотивации к работе.

* Сотрудники работают на конкурента.

Потеря конкурентного преимущества, утечка коммерческой информации, нанесение ущерба репутации компании.

* Сотрудник хочет создать собственную конкурентную компанию.

Потеря ключевых сотрудников, риски конфликта интересов, возможная утечка коммерческой информации.

* Сотрудники распространяют государственную тайну.

Штрафы, уголовная ответственность, потеря доверия со стороны клиентов и партнеров.

* Используется потенциально опасное ПО, содержащее уязвимости.

Утечка данных, вирусы, взлом, повреждение IT-инфраструктуры.

* Административные пароли передаются по открытым каналам.

Незаконное доступ к системам, изменение конфигураций без согласия, возможность взлома.

* Бреши в межсетевом периметре компании.

Утечка данных, несанкционированный доступ к внутренней сети, возможность атак хакеров.

* Оставлены закладки в самописном программном обеспечении.

Утечка конфиденциальной информации, возможность несанкционированного доступа к данным.

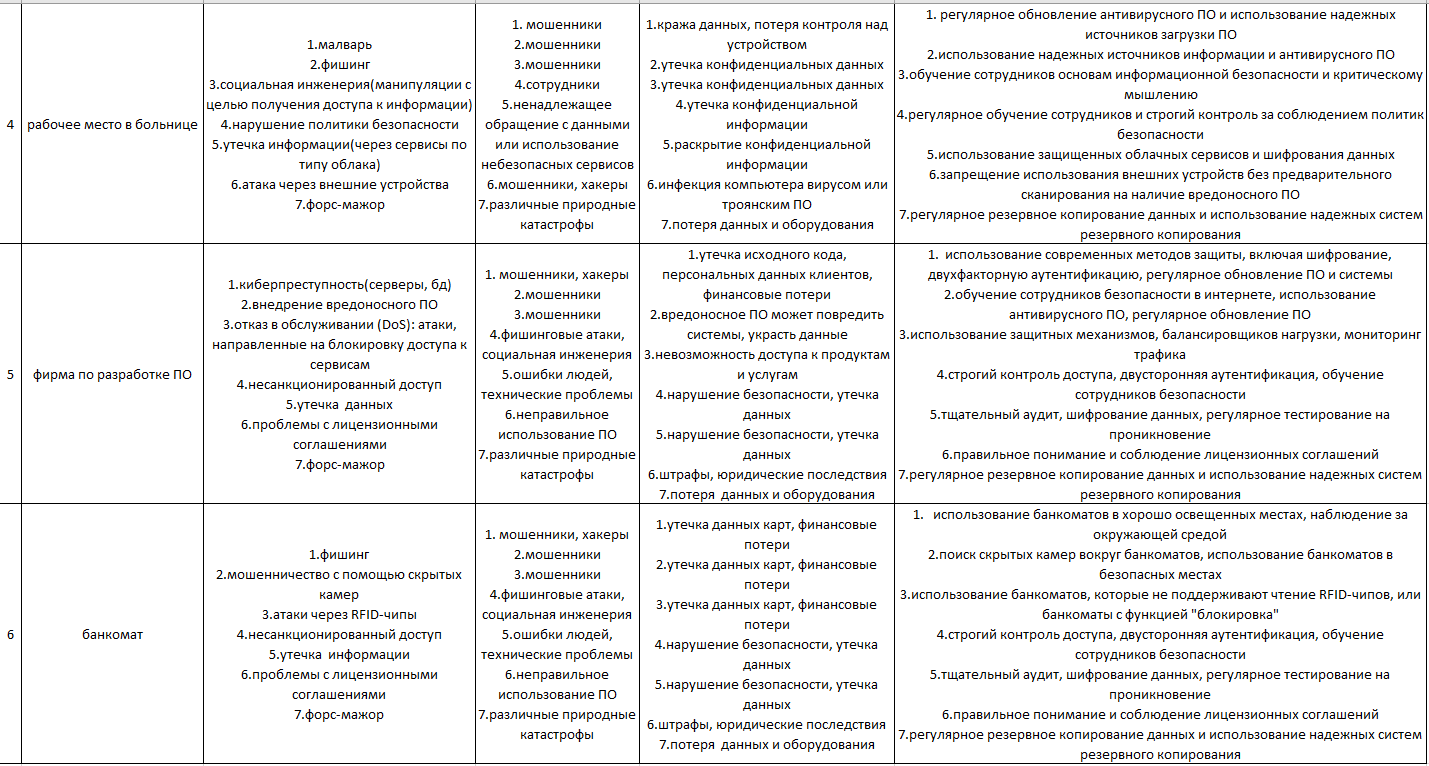
1. Как предотвратить потерю информации?

* Регулирование использования интернета и игровых приложений во время рабочего времени.
* Обучение ответственности за выполнение своих обязанностей и распределение задач.
* Регулярное обучение сотрудников по вопросам информационной безопасности и конфиденциальности.
* Запрет на совмещение работы с другими должностями без разрешения руководства.
* Обеспечение прозрачности и честности в отношениях между сотрудниками и компанией.
* Разработка и соблюдение политики конфиденциальности и защиты интеллектуальной собственности.
* Тщательное расследование инцидента, применение юридических мер в соответствии с законодательством.
* Регулярное обновление ПО, использование антивирусных решений, обучение безопасному использованию компьютеров.
* Использование сильных паролей, шифрование передачи паролей, использование централизованного управления доступом.
* Регулярное сканирование на наличие уязвимостей, использование межсетевого экрана, обучение безопасности.
* Удаление закладок, аудит использования ПО, обучение безопасности.

1. Что следует предпринять для устранения данных нарушений?

* Мониторинг использования ресурсов и проведение обучения по этическим нормам поведения на рабочем месте.
* Разработка системы обратной связи и оценки эффективности исполнения обязанностей.
* Изменение всех паролей, аудит системы управления доступом, обучение сотрудников принципам безопасности.
* Закрытие обнаруженных уязвимостей, усиление мер безопасности, мониторинг активности в сети.
* Изолирование и удаление вредоносного ПО, восстановление системы после атаки.

**Задание 3.**

Заполните таблицу. Для каждого из этих объектов указать не менее 7 угроз, которые могут быть реализованы по отношению к обрабатываемой в них информации, а также методы борьбы с данными угрозами. Обозначить источник каждой из приведенных угроз.