**Практическая работа Тестирование безопасности**

**Фахрутдинова Елизавета ИСиП301**

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

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

* Угрозы компании: Снижение производительности, риск утечки конфиденциальной информации, увеличение расходов на оплату труда без соответствующего возврата.
* Предотвращение потери информации: Внедрение политики использования интернета на рабочем месте, мониторинг интернет-активности сотрудников, фильтрация доступа к определенным категориям сайтов.
* Устранение нарушения: Обучение сотрудников правилам использования интернета на рабочем месте, установка программного обеспечения для мониторинга и ограничения доступа к развлекательным сайтам.

1. Нарушение 2: Играют в игры на работе.

* Угрозы компании: Уменьшение производительности, отвлечение от рабочих задач, повышенный риск возникновения ошибок из-за невнимательности.
* Предотвращение потери информации: Установка программного обеспечения для блокировки доступа к игровым ресурсам на рабочих компьютерах, обучение сотрудников корпоративным правилам.
* Устранение нарушения: Строгая политика безопасности, мониторинг активности на рабочих компьютерах, введение дисциплинарных мер.

1. Нарушение 3: Перекладывают свои обязанности на других.

* Угрозы компании: Неравномерное распределение нагрузки, снижение эффективности работы коллектива, риск конфликтов и недовольства среди сотрудников.
* Предотвращение потери информации: Разработка четкой системы ответственности, регулярные отчеты о выполнении задач, обучение сотрудников эффективному управлению временем и задачами.
* Устранение нарушения: Проведение переговоров с сотрудниками, выявление причин перекладывания обязанностей, распределение задач с учетом специализации и загруженности.

1. Нарушение 4: Сотрудники копируют конфиденциальные данные компании.

* Угрозы компании: Утечка конфиденциальной информации, нарушение доверия клиентов и партнеров, финансовые потери, угроза репутации.
* Предотвращение потери информации: Реализация строгих правил доступа к конфиденциальным данным, мониторинг активности пользователей, шифрование конфиденциальной информации.
* Устранение нарушения: Проведение внутреннего расследования, выявление виновных, ужесточение правил доступа к конфиденциальной информации, обучение сотрудников правилам конфиденциальности.

1. Нарушение 5: Сотрудники одновременно работают на другой работе.

* Угрозы компании: Снижение производительности, разрыв рабочего процесса, возможное разглашение конфиденциальной информации, нарушение трудовой дисциплины.
* Предотвращение потери информации: Мониторинг рабочей активности сотрудников, разработка политики запрета на дополнительную работу во время рабочего дня, контроль за использованием корпоративных ресурсов.
* Устранение нарушения: Проведение беседы с сотрудниками, уточнение корпоративных правил, назначение дополнительных обязанностей для предотвращения свободного времени.

1. Нарушение 6: Сотрудники работают на конкурента.

* Угрозы компании: Утечка конфиденциальной информации, утрата конкурентного преимущества, финансовые потери, угроза репутации.
* Предотвращение потери информации: Строгие ограничения доступа к конфиденциальным данным, контроль за перемещением сотрудников к конкурентам, подписание сотрудниками неразглашения конфиденциальной информации.
* Устранение нарушения: Проведение расследования, применение дисциплинарных мер, изменение политики безопасности.

1. Нарушение 7: Сотрудник хочет создать собственную конкурентную компанию.

* Угрозы компании: Утечка конфиденциальной информации, утрата ключевых кадров, конкуренция на рынке, финансовые потери.
* Предотвращение потери информации: Заключение сотрудниками соглашений о неразглашении конфиденциальной информации, контроль за перемещением ключевых кадров, мониторинг активности сотрудников.
* Устранение нарушения: Проведение переговоров с сотрудником, предложение альтернативных возможностей внутри компании, при необходимости - применение юридических мер.

1. Нарушение 8: Сотрудники распространяют государственную тайну.

* Угрозы компании: Потеря доверия со стороны государства, правовые преследования, финансовые и репутационные потери.
* Предотвращение потери информации: Строгие правила доступа к государственным данным, мониторинг активности сотрудников, обучение сотрудников правилам обработки государственной информации.
* Устранение нарушения: Проведение расследования, сотрудничество с правоохранительными органами, изменение политики безопасности.

1. Нарушение 9: Используется потенциальное опасное ПО, содержащее уязвимости, позволяющие скрытую передачу данных, дающие возможность деструктивного влияния на ИТ инфраструктуру компании.

* Угрозы компании: Утечка конфиденциальной информации, нарушение целостности и доступности ИТ инфраструктуры, финансовые потери, угроза репутации.
* Предотвращение потери информации: Регулярное обновление программного обеспечения, мониторинг сетевой активности, установка антивирусного и антишпионского ПО.
* Устранение нарушения: Выявление и удаление опасного ПО, усиление мер безопасности, обучение сотрудников правилам работы с информационными ресурсами.

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

* Угрозы компании: Несанкционированный доступ к информации, нарушение целостности и доступности ИТ инфраструктуры, угроза конфиденциальности данных.
* Предотвращение потери информации: Использование шифрования при передаче паролей, ограничение доступа к административным ресурсам, регулярное изменение паролей.
* Устранение нарушения: Изменение политики безопасности, обучение сотрудников правилам безопасного обращения с административными паролями, применение многофакторной аутентификации.

1. Нарушение 11: Администраторы сделали бреши в межсетевом периметре компании для удобства.

* Угрозы компании: Утечка конфиденциальной информации, несанкционированный доступ к ИТ инфраструктуре, угроза целостности и доступности данных.
* Предотвращение потери информации: Проведение аудита безопасности, закрытие обнаруженных уязвимостей, внедрение средств мониторинга и обнаружения вторжений.
* Устранение нарушения: Восстановление межсетевого периметра, изменение политики безопасности, обучение администраторов правилам безопасности.

1. Нарушение 12: Оставлены закладки в самописном программном обеспечении.

* Угрозы компании: Несанкционированный доступ к данным, утечка конфиденциальной информации, нарушение целостности программного кода.
* Предотвращение потери информации: Аудит кода программного обеспечения, обучение разработчиков правилам безопасного программирования, использование средств контроля версий.
* Устранение нарушения: Удаление закладок из программного кода, разработка процедур проверки кода перед выпуском в эксплуатацию, обновление программного обеспечения.

**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.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Банковская карта | Атака прерывания | Внешний хакер | Потеря денег, мошенничество | Использование защищенных соединений, мониторинг банковских операций |
|  | Атака отказа в обслуживании | Внутренний персонал | Невозможность осуществления банковских операций | Регулярное обновление систем, резервное копирование данных |
|  | Атака перехвата | Вредоносное ПО | Кража данных, мошенничество | Использование антивирусного ПО, шифрование данных |
|  | Атака на целостность | Злоумышленники | Изменение баланса, потеря доверия клиентов | Установка механизмов контроля целостности данных |
|  | Атака на сессии | Компьютерные вирусы | Несанкционированный доступ к аккаунту | Использование механизмов многофакторной аутентификации |
|  | Атака на инфраструктуру | Хакерская группировка | Недоступность банковских услуг | Регулярное обновление систем безопасности, мониторинг сетевой активности |
|  | SQL-инъекции | Хакер | Получение конфиденциальной информации | Использование параметризованных запросов, фильтрация ввода данных |
| Рабочее место директора | Атака прерывания | Конкуренты | Утечка конфиденциальной информации | Использование защищенных средств связи, мониторинг сетевой активности |
|  | Атака отказа в обслуживании | Внутренний персонал | Невозможность доступа к важным данным | Регулярное обновление систем, резервное копирование данных |
|  | Атака перехвата | Киберпреступники | Утечка конфиденциальной информации | Использование криптографических средств защиты, обучение персонала правилам безопасности |
|  | Атака на целостность | Злоумышленники | Изменение или подделка документов | Установка механизмов контроля целостности данных, ограничение доступа |
|  | Атака на сессии | Внутренн ий персонал | Несанкционированный доступ к конфиденциальным данным | Использование механизмов аутентификации и авторизации |
|  | Атака на инфраструктуру | Внешние хакеры | Нарушение работы информационной системы | Регулярное обновление систем безопасности, мониторинг сетевой активности |
|  | Х55 (межсайтов ый) | Злоумышленники | Внедрение вредоносного кода на рабочие станции | Фильтрация ввода данных, использование механизмов защиты браузера |
| Домашний компьютер | Атака прерывания | Киберпреступники | Удаленное управление компьютером | Использование сетевых брандмауэров, мониторинг сетевой активности |
|  | Атака отказа в обслуживании | Вредоносное ПО | Потеря данных | Регулярное создание резервных копий, использование антивирусного ПО |
|  | Атака перехвата | Вредоносное ПО | Кража личных данных | Использование криптографических средств защиты, обновление программного обеспечения |
|  | Атака на целостность | Хакерская группировка | Изменение или уничтожение данных | Использование механизмов контроля целостности данных, ограничение доступа |
|  | Атака на сессии | Киберпреступники | Удаленный доступ к личным данным | Использование механизмов аутентификации и авторизации, мониторинг сетевой активности |
|  | Атака на инфраструктуру | Хакеры | Нарушение работы домашней сети | Защита \/-А! сети, обновление маршрутизатора и антивирусного ПО |
|  | Sql-инъекции | Хакер | Несанкционированный доступ к данным | Использование параметризованных запросов, фильтрация ввода данных |
| Рабочее место в больнице | Атака прерывания | Внешний хакер | Недоступность медицинских данных | Регулярное обновление систем безопасности, контроль доступа к данным |
|  | Атака отказа в обслуживании | Внутренний персонал | Невозможность доступа к медицинским данным | Резервное копирование данных, обучение персонала правилам безопасности |
|  | Атака перехвата | Внутренний персонал | Утечка медицинских данных | Шифрование медицинских данных, мониторинг доступа к данным |
|  | Атака на целостность | Злоумышленники | Изменение медицинских записей | Использование механизмов контроля целостности данных, ограничение доступа |
|  | Атака на сессии | Внутренний персонал | Несанкционированный доступ к медицинским данным | Использование механизмов аутентификации и авторизации |
|  | Атака на инфраструктуру | Внешний хакер | Нарушение работы медицинской системы | Регулярное обновление систем безопасности, мониторинг сетевой активности |
| Фирма по разработке ПО | Атака прерывания | Конкуренты | Потеря интеллектуальной собственности | Использование защищенных средств связи, контроль доступа к данным |
|  | Атака отказа в обслуживании | Внутренний персонал | Невозможность доступа к разработке ПО | Регулярное обновление систем, резервное копирование данных |
|  | Атака перехвата | Киберпреступники | Утечка кода ПО | Использование криптографических средств защиты, обучение персонала правилам безопасности |
|  | Атака на целостность | Злоумышленники | Изменение или уничтожение исходного кода | Использование механизмов контроля версий, ограничение доступа |
|  | Атака на сессии | Внутренний персонал | Несанкционированный доступ к исходному коду | Использование механизмов аутентификации и авторизации |
|  | Атака на инфраструктуру | Внешние хакеры | Нарушение работы разработки ПО | Регулярное обновление систем безопасности, мониторинг сетевой активности |
|  | Х55 (межсайтовый) | Злоумышленники | Внедрение вредоносного кода в разрабатываемое по | Фильтрация ввода данных, использование механизмов защиты браузера |
| Банкомат | Атака прерывания | Киберпреступники | Недоступность банковских услуг | Мониторинг сетевой активности, регулярное обновление систем |
|  | Атака отказа в обслуживании | Внутренний персонал | Невозможность осуществления банковских операций | Резервное копирование данных, использование защищенных соединений |
|  | Атака перехвата | Внутренний персонал | Кража конфиденциальных данных | Шифрование данных, мониторинг сетевой активности |
|  | Атака на целостность | Хакерская группировка | Изменение баланса или уничтожение денежных средств | Использование механизмов контроля целостности данных, ограничение доступа |
|  | Атака на сессии | Киберпреступники | Несанкционированный доступ к банковскому счету | Использование механизмов аутентификации и авторизации |
|  | Атака на инфраструктуру | Хакеры | Нарушение работы банкоматов | Регулярное обновление систем безопасности, мониторинг сетевой активности |