МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
Московский государственный университет геодезии и картографии
(МИИГАиК)

О Т Ч Е Т
№ 3

по курсу
ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

на тему
РАЗРАБОТКА ПАМЯТКИ ВВОДНОГО ИНСТРУКТАЖА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Выполнил: студент 2024-ФГИИБ-ПИ-1б
Бондаренко Максим Юрьевич
Проверил: преподаватель кафедры ИИС
Пучин В.А.

Москва, 2024

Памятка по курсу “Основы Информационной Безопасности”

Тема:

Вводный инструктаж по информационной безопасности для нового сотрудника.

Введение в информационную безопасность :

1. Понятие информационной безопасности

Информационная безопасность (ИБ) — это комплекс мер для защиты данных от несанкционированного доступа, утраты и компрометации.

2. Почему важна ИБ в компании

Сохранение данных, соблюдение конфиденциальности и защита от кибер-угроз помогают компании сохранять конкурентное преимущество и доверие клиентов.

3. Основные угрозы информационной безопасности

Основные угрозы — это утечка данных, взломы, фишинг и вирусные атаки. Знание угроз позволяет сотруднику осознанно подходить к их предотвращению.

Политики безопасности и ответственность сотрудников :

4. Политика работы с устройствами

• Используются только корпоративные устройства или устройства, одобренные ИТ-отделом.

5. Политика доступа к данным

Доступ предоставляется только тем сотрудникам, которые непосредственно работают с определенными данными.

6. Правила работы с корпоративными данными

Запрещается передавать конфиденциальную информацию третьим лицам и сохранять ее на устройствах вне компании.

Работа с устройствами и данными :

7. Безопасная работа с устройствами

Не оставляйте устройства без присмотра, блокируйте экран, уходя от компьютера, и не используйте личные устройства для рабочих целей без разрешения.

8. Шифрование и защита данных

Шифрование данных защищает их от несанкционированного доступа. Используйте шифрование для хранения и передачи конфиденциальных данных.

9. Защита съемных носителей

Использование флеш-накопителей может нести риск заражения. Подключайте только разрешенные устройства и сканируйте их на вирусы.

Аутентификация и доступ :

10. Многофакторная аутентификация (MFA)

MFA значительно повышает уровень защиты аккаунтов, требуя подтверждения входа с помощью дополнительных факторов.

11. Использование уникальных и сложных паролей

Создавайте пароли из случайных символов и не используйте одинаковые пароли для разных сервисов. Рекомендуется использовать менеджеры паролей.

12. Права доступа и необходимость ограничений

Каждый сотрудник должен иметь доступ только к тем данным и системам, которые необходимы для выполнения рабочих задач.

Предотвращение кибератак и фишинга :

13. Что такое фишинг и как его распознать

Фишинг — это попытка обманом заставить сотрудника раскрыть конфиденциальную информацию. Не открывайте ссылки и файлы из подозрительных писем.

14. Признаки фишинговых писем и сайтов

Признаки фишинга: ошибки в тексте, неофициальные адреса отправителей, срочные запросы на предоставление данных.

15. Сообщение о подозрительных действиях

Если получили подозрительное письмо или заметили что-то необычное, сообщите об этом в службу ИБ компании.

Поддержание безопасности на высоком уровне :

16. Регулярное обновление ПО и антивирусов

Устаревшее ПО и антивирусные базы — распространенная уязвимость. Регулярные обновления защищают устройства от новых угроз.

17. Внимательное отношение к собственным действиям

Поддержание ИБ требует внимательности. Сотруднику важно быть осторожным и осознанно подходить к работе с информацией и технологиями.