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 2025–ФГиИБ–ПИ-2б
Грязнов Егор Иванович
Проверил: преподаватель кафедры ИИС
Пучин В.А.

Москва, **2025**

Задание

1. Изучить требования к проведению вводного инструктажа по информационной безопасности (законодательные и нормативные документы, внутренние регламенты организаций).
2. Сформировать структуру памятки, включающую:
   - цели инструктажа;
   - основные угрозы информационной безопасности;
   - правила работы с компьютером (в офисе и не офисе);
   - правила безопасного обращения с учетными записями и паролями;
   - правила работы с электронной почтой и интернет-ресурсами;
   - предупредить про системы слежения;
   - порядок действий при обнаружении подозрительных ситуаций (фишинг, вредоносное ПО, утечка информации и т.д.);
   - политика «чистого» стола;
   - ответственность сотрудников за нарушение требований.
3. Объем – 1–2 страницы, но не менее 20 пунктов. Стиль изложения – краткий, понятный для пользователя без специальной подготовки.

Оформление: ответ на задание должен быть представлен после заголовка «Памятка» и выглядеть в формате списка, соответствующего структуре, описанной выше. Текст должен быть в формате **Times New Roman**, размер **14**, выравнивание по **ширине**, абзац с отступом **1.25 см**, междустрочный интервал **1.5 строки**, без выделений (жирным, курсивом, подчеркнутый).

Памятка

- Цели инструктажа:

1. Довести до сведения каждого сотрудника основные правила информационной безопасности, чтобы минимизировать риски для компании, защитить конфиденциальную информацию и обеспечить непрерывность бизнес-процессов.

- Основные угрозы информационной безопасности:

2. Социальная инженерия: Манипулирование людьми с целью получения конфиденциальной информации (паролей, данных карт).

3. Фишинг: Поддельные письма и сайты, имитирующие легитимные, для кражи учетных данных.

4. Вредоносное программное обеспечение (ПО): Вирусы, трояны, программы-шифровальщики, которые могут украсть или заблокировать данные.

5. Неавторизованный доступ: Попытки получить доступ к данным или системам без соответствующих прав.

6. Утечка информации: Случайное или умышленное разглашение конфиденциальных данных.

- Правила работы с компьютером (в офисе и не в офисе):

7. Все рабочие компьютеры должны быть защищены сложными паролями и блокироваться при каждом выходе из рабочего места.

8. Установка любого программного обеспечения на рабочие ПК должна быть согласована с отделом информационной безопастности.

9. Запрещается использовать непроверенные внешние носители (флешки, HDD) на рабочих ПК.

10. При работе вне офиса (удаленно) используйте только защищенное VPN-соединение, предоставленное компанией.

11. Не оставляйте рабочий ноутбук или мобильные устройства без присмотра в общественных местах.

12. Обезопасьте ваш экран от посторонних взглядов.

13.Съёмные носители не используйте без разрешения.

- Правила безопасного обращения с учетными записями и паролями:

14. Используйте уникальные сложные пароли (не менее 8 символов, заглавные/строчные буквы, цифры, спецсимволы).

15. Запрещается использовать один и тот же пароль для рабочих и личных учетных записей.

16. Никогда и никому не сообщайте свои пароли, даже коллегам или лицам, представляющимся IT-специалистами.

17. Немедленно меняйте пароль, если есть подозрение, что он был скомпрометирован.

18. Используйте многофакторную аутентификацию (MFA/2FA) везде, где это возможно.

- Правила работы с электронной почтой и интернет-ресурсами:

19. Не открывайте вложения и не переходите по ссылкам в письмах от неизвестных отправителей.

20. Всегда проверяйте адрес отправителя и ссылки (наводя курсор) перед кликом.

21. Не используйте корпоративную электронную почту для регистрации на непроверенных ресурсах.

22.Остерегайтесь писем с срочными требованиями или подозрительными предложениями (например, «вы выиграли приз»).

23. Не выпускайте запароленные письма и не впускайте(без проверки СБ).

24.Проверка антиспама(SPF)

25. Слишком большой по размеру файл предавайте СБ, после загружайте в облако.

- Системы слежения:

26. Компания вправе осуществлять мониторинг использования корпоративных ресурсов (трафик, почта, рабочие ПК) в целях обеспечения безопасности. Это предусмотрено внутренними регламентами и законодательством.

- Действия при обнаружении подозрительных ситуаций:

27.Определите фишинговое письмо: посмотрите на адрес отправителя, проверьте вероятность такого сообщения, подумайте ожидаете ли вы такое письмо.

28. При получении фишингового письма: Не отвечайте на него, не переходите по ссылкам. Немедленно сообщите в IT-отдел/службу безопасности и удалите его.

29. При подозрении на заражение ПО: Немедленно отключите компьютер от сети (интернета и локальной) и сообщите в IT-отдел.

30. При утечке информации: Немедленно сообщите своему руководителю и в службу безопасности. Зафиксируйте, какая информация и при каких обстоятельствах была раскрыта.

31. При запросе конфиденциальной информации от «руководства» по телефону или в мессенджере: Прекратите разговор и перезвоните по официальному номеру телефона, чтобы подтвердить личность и запрос.

- Политика «чистого» стола:

32. Не оставляйте на рабочем столе документы с конфиденциальной информацией (отчеты, переписка, пароли) без присмотра.

33. Все физические носители с важной информацией должны храниться в запертых ящиках.

34. Очищайте рабочее место в конце дня.

35. Всегда блокируйте компьютер (Win+L), даже если отходите на несколько минут.

- Ответственность сотрудников за нарушение требований:

36. Нарушение правил информационной безопасности влечет за собой дисциплинарную ответственность вплоть до увольнения, а в случаях, предусмотренных законом, - административную или уголовную ответственность.

С памяткой ознакомлен(а): Подпись: