

**ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ ЗАЩИТЫ ПРАВ
ПОТРЕБИТЕЛЕЙ И БЛАГОПОЛУЧИЯ ЧЕЛОВЕКА
ПО ЧЕЧЕНСКОЙ РЕСПУБЛИКЕ**
Управление Роспотребнадзора по Чеченской Республике

Протокол совещания

**«Разъяснения по реализации мероприятий во исполнение Указа
Президента Российской Федерации от 01.05.2022 №250 «О
дополнительных мерах по обеспечению информационной безопасности
Российской Федерации»».**

15.08.2022г.

г. Грозный

Председатель: Р.М. Термулаева – руководитель Управления Роспотребнадзора по Чеченской Республике (далее Управление), Главный государственный санитарный врач по Чеченской Республике.

Присутствовали: начальники отделов и территориальных отделов Управления.

Выступили: заместитель начальника отдела организации и обеспечения деятельности и социально-гигиенического мониторинга Дацаева Л.С.

С 01.05.2022 вступил в силу Указ Президента Российской Федерации от №250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

На повестке дня: разъяснение основных вопросов по информационной безопасности в Управлении Роспотребнадзора по Чеченской Республике (далее Управление), обработки и защиты конфиденциальной информации, в том числе и персональных данных. Знакомство с нормативно –методической базой в области защиты персональных данных и с вопросами организации конфиденциального делопроизводства, узнают о способах и средствах его защиты.

1. Основные понятия, термины и определения в области защиты информации. Основные направления и составные части системы защиты информации.

2. Законодательная и нормативная база правового регулирования защиты информации.

3. Мероприятия по защите информации. Противодействие промышленному шпионажу.

Источники угрозы информации. Защита информации от утечки по техническим каналам: технические средства защиты. Человеческий фактор: работа по предупреждению утечки информации по этому каналу.

4. Методы и средства защиты компьютерных систем. Возможные способы утери, искажения, изменения компьютерной информации или получения к ней несанкционированного доступа; вирусная угроза компьютерной информации. Защита информации при работе в сети Internet: межсетевое экранирование; основы криптографической защиты информации; стеганография. VPN (виртуальная частная сеть): преимущества организации виртуальных частных сетей на основе Internet. Практические примеры применения криптографических методов защиты информации.

5. Аудит информационной безопасности и разработка политики информационной безопасности в компании. Анализ внутренних и внешних угроз информационной безопасности службы. Методика разработки политики информационной безопасности в Управлении.

Международные и российские стандарты безопасности информационных систем (ISO 17799, ГОСТ Р ИСО/МЭК 17799-2005).

6. Организация работы Службы информационной безопасности (СИБ) предприятия: практический опыт. Процедура создания СИБ на предприятии. Разделение функций между СИБ и IT-подразделением. Место СИБ в структуре предприятия. Организация взаимодействия с Руководством и руководителями структурных IT-подразделений Управления.

7. Коммерческая тайна. Понятие "коммерческой тайны" в предпринимательской деятельности. Законодательство РФ в области защиты коммерческой тайны. Методика составления Перечня сведений, содержащих коммерческую тайну. Внутренние нормативные документы, регламентирующие деятельность компании в области защиты коммерческой тайны.

8. Организация защиты персональных данных. Международное и российское законодательство в области обработки персональных данных; общие вопросы их обработки и обеспечения защиты в Управлении, порядок проведения работ. Согласование документов с регуляторами.

Обзор основных мероприятий и программно-аппаратных средств защиты информации, применяемых при создании системы защиты персональных данных.

9. Конфиденциальное делопроизводство Управления. Принципы построения конфиденциального делопроизводства службы, создание нормативных документов для обеспечения его функционирования. Порядок его взаимодействия с открытым делопроизводством. Служба конфиденциального делопроизводства Управления, ее организационные формы, штатный состав и численность работников. Конфиденциальный документооборот и конфиденциальное информационное хранилище как составные части системы конфиденциального делопроизводства. Порядок создания документов. Грифы конфиденциальности: порядок присвоения и снятия, сроки действия.

Электронная цифровая подпись как базовый механизм обеспечения юридической силы документа при электронном документообороте.

10. Системы защиты конфиденциального делопроизводства Управления. Основные направления и технические средства защиты материальных и электронных конфиденциальных документов.

Участники семинара обеспечены **информационно-справочными материалами** по тематике семинара.

Секретарь

Хаджиева З.Х.

