Протокол самостоятельной работы

По Теории Защиты Информации

На тему: Защита информации в Румынии

Выполнил студент К17.1

Шишелов Владимир

**Введение**

Задача работы состоит в описании современных методов защиты информации на государственном уровне, такие как правовое законодательство в категории защиты информации, требование к аппаратному и программному обеспечению и другие. В протоколе описываются методы защиты информации в Румынии.

Важно учитывать, что Румыния входит в ряд мировых альянсов и придерживается многих законов, и правил в сфере защиты информации созданных этими альянсами.

**Обработка и защита персональной информации**

Национальный надзорный орган за обработкой персональных данных, как автономный центральный государственный орган с общей компетенцией в области защиты персональных данных, представляет собой гарант соблюдения основных прав на частную жизнь и защиту персональных данных, особенно предусмотренных Статьи 7 и 8 Хартии основных прав Европейского Союза, статья 16 Договора о функционировании Европейского Союза и статья 8 Европейской конвенции о защите прав человека и основных свобод.

2016 год знаменует собой ключевой момент в эволюции европейских правил защиты персональных данных путем принятия Европейским парламентом и Советом постановления о защите физических лиц в отношении обработки персональных данных и бесплатного использования. перемещение таких данных (Общее положение о защите данных), имеющее прямое применение во всех государствах-членах Европейского Союза по состоянию на 25 мая 2018 года, вместе с принятием Директивы о защите данных, обрабатываемых с целью предотвращения, обнаружения, расследование и судебное преследование преступлений и другая судебная деятельность.

Для учреждений эта реформа нормативной базы в данной области подразумевает в краткосрочной перспективе комплексную оценку конкретных инструментов для обеспечения защиты персональных данных с целью адаптации национальной нормативной базы и институциональной подготовки к применению новые европейские правила, в том числе с точки зрения достижения эффективного сотрудничества с Европейским советом по защите данных и другими соответствующими органами в Европейском союзе.

Таким образом, укрепление административного потенциала Управления является приоритетом и требует выделения адекватных материальных, финансовых и человеческих ресурсов для выполнения наших новых конкретных задач, для эффективного применения стандартов Европейского Союза, предусмотренных в новых принятых правилах.

Деятельность учреждений должна соответствовать требованиям соблюдения правил обработки персональных данных в публичной и частной сфере, чтобы достичь желаемого, чтобы обеспечить реальное осуществление.

**Переработка криминального кодекса в связи с вступлением в ЕС касательно Защиты Информации**

Одним из важнейших изменений в кодекс было внесение криминальной отвествинности за утерю или продажу не только государственных, а корпоративных данных.

Одним из этих законов является закон номер 169 ч.2:

«Разглашение определенных документов или данных, составляющих государственную тайну, или других документов или данных лицом, которое знает эти данные и документы в связи с его обязанностями, если действие имеет характер угрозы безопасности государства, наказывается лишение свободы на срок от 7 до 15 лет и нарушение определенных прав.  
Хранение вне служебных обязанностей документа, составляющего государственную тайну, если действие имеет характер угрозы безопасности государства, -наказывается лишением свободы на срок от 5 до 10 лет.  
Штраф, предусмотренный в параграфе 2, применяется к хранению вне служебных обязанностей других документов, предназначенных для раскрытия, если действие имеет характер угрозы безопасности государства .  
Если любое другое лицо совершает действия, упомянутые в предыдущих параграфах, наказывается тюремным заключением на срок от 1 до 7 лет ».

И закон 252 ч.1:

 Халатность, ведущая к уничтожению, изменению, утрате или изъятию документа, представляющего государственную тайну, и халатность, которая приводит к раскрытию другим лицом такой тайны, если она  
наносит ущерб государственным интересам, наказываются сроком от 3 месяцев до 3 лет. тюрьма.

**Роль ЕС в информационной безопасности Румынии**

После ассоциации Румынии был выдвинут ряд требований касательно ЗИ. Важнейшим было использование оборудования и ПО сертифицированного международной организацией ориентированной на защите информации и кибербезопасности – NCF.

Также ЕС профинансировало создание государственных структур в министерстве обороны и внутренних дел, направленных на защиту информационного пространства в Румынии.

**Вывод**

Румыния имеет средства и умения для борьбы с кибератаками как на государственном уровне так и на уровне граждан и их личной информации, а помощь союзников и их влияние на законодательство страны хорошо выражается в развитии киберзащиты Румынии.