Тема 1.1 Законодательство в области информационной безопасности

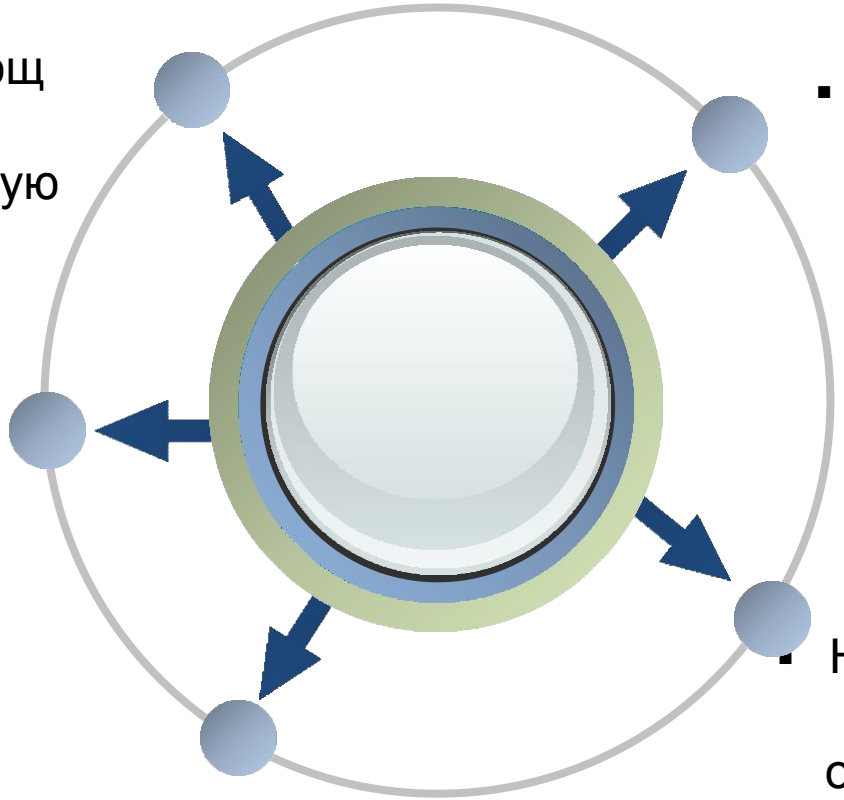
ЦАТЭК Усатова О.А.

С момента приобретения независимости Республики Казахстан первый президент Нурсултан Абишевич Назарбаев неоднократно акцентировал внимание на необходимость защиты интересов граждан в Республике Казахстан. Так, в Послании Президента страны народу Казахстана от 10 октября 1997 года «Казахстан – 2030. Процветание, безопасность и улучшение благосостояния всех казахстанцев» долговременным приоритетом установлена государственная защищенность, где одним из важных направлений является информационная безопасность.

Комплексный механизм процессов обеспечения информационной безопасности нашей Республики охватывает организационные, социальные, технические и программные подходы, способные осуществлять конституционные права и свободу человека, гражданина в области получения информации, пользования ею в целях защиты конституционного строя, суверенитета и территориальной целостности Республики Казахстан, финансовой, а также общественной устойчивости, формирование выгодного интернационального партнерства в сфере информативной защищенности.

Проблемные вопросы

- нормативные документы, регламентирующих их информационную безопасность
- Отсутствие единого стандарта по информационной безопасности
- Отсутствие квалифицированных кадров по информационной безопасности
- Отсутствие контролирующего и уполномоченного государственного органа по информационной безопасности
- Неопределенность зоны ответственности за нарушение информационной безопасности



Нормативно-правовые аспекты

- Закон РК «Об информатизации»
- Закон РК «О доступе к информации»
- Закон РК «О персональных данных и их защите»
- Закон РК «О национальной безопасности РК»
- Концепция «Киберщит Казахстана»
- Декабрь 2016 года Правительство РК №832 «Об утверждении требований к обеспечению единых информационно-коммуникационных технологий и информационной безопасности»

Принятый **6 января 2012 года Закон «О национальной безопасности Республики Казахстан»** содержит необходимые статьи, в них даны чёткие определения с позиции государства, затрагивающих вопросы информационной безопасности страны в целом и граждан в частности.

На законодательном уровне в Республике Казахстан формируется и закрепляется национальная концепция обеспечения информационной безопасности, электронного документооборота, автоматизированных информационных систем, ресурсов, ИКТ, а также важных объектов.

При построении и эксплуатации телекоммуникационных сетей связи необходимо учитывать требования Республики Казахстан о соблюдении национальной безопасности в области связи. Об этом свидетельствует последняя действующая поправка статьи «О полномочиях государственных органов Республики Казахстан» от 27 декабря 2017 года.

21 мая 2013 года был принят закон Республики Казахстан (РК) **№ 94–V «О персональных данных и их защите»** (с изменениями и дополнениями по состоянию на 28.12.2017 г.), в нем регулируются отношения, связанные со сбором и обработкой, а также защитой персональных данных. Не маловажными являются Закон РК от 24 ноября 2015 года **№ 418–V «Об информатизации»** (с изменениями по состоянию на 01.01.2020 г.) и Закон РК от 7 января 2003 года **№ 370–II «Об электронном документе и электронной цифровой подписи»** (с изменениями по состоянию на 25.11.2019г.).

В Республике Казахстан 12 декабря 2017 года, Постановлением Правительства **№827 была утверждена программа государства «Цифровой Казахстан»**. В данной программе основным аспектом является развитие экономики страны и повышение жизнедеятельности населения, основанной на совершенствовании и ускорении развития инфокоммуникационных технологий и также создание цифровой экономики. Основное внимание уделено обеспечению информационной безопасности в сфере информационно-коммуникационных технологий и консолидации кибербезопасности автоматизированных информационных систем в нашей стране.

С развитием технологического прогресса и общего уровня информатизации появляются также и новые угрозы. Киберпреступность позволяет злоумышленникам совершать противоправные и незаконные действия, находясь в тысячах километрах от цели их атаки. В Послании народу Казахстана «Третья модернизация Казахстана: Глобальная конкурентоспособность» Президент Республики Казахстан отмечал, что все большую актуальность приобретает борьба с киберпреступностью. В связи с этим была разработана и утверждена Постановлением Правительства Республики Казахстан от 30 июня 2017 года **№407 Концепция кибербезопасности («Киберщит Казахстана»)**, в ней определены основные направления реализации государственной политики в сфере защиты электронных информационных ресурсов, информационных систем и сетей телекоммуникаций, обеспечения безопасного использования ИКТ.

Ключевые направления

Построение защищенной инфраструктуры

Обеспечения информационной безопасности систем

Обеспечение защиты данных, в том числе

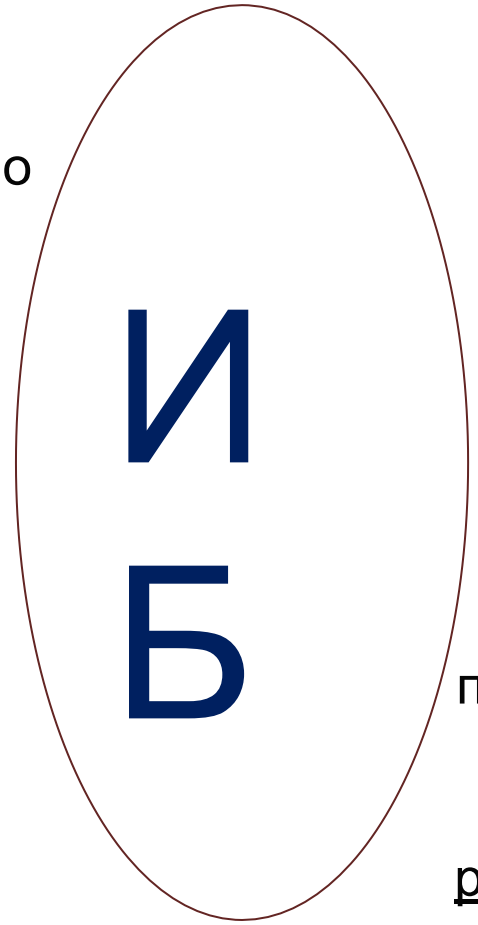
персональных

Подготовка специалистов в данной области

(ИБ) Казахстанское производство оборудования

Практические мероприятия

- Изучение нормативно прав. аспектов
- Проведение организационных мероприятий
- Проведение аудита по ИБ
- Проведение инвентаризации Информационных систем, оборудования и ПО
- Разработка документации (Политики ИБ, Инструкций, руководства пользователей, планов, отчетов, журналов)



- Проведение обучения пользователей
- Разработка дорожной карты по устранению нарушений, выявленных при аудите
- Тестирование информационных систем по требованиям ИБ
- Ввод в промышленную эксплуатацию информационных систем, приложений, ресурсов

Защита информационных систем организаций образования

***Примечание**: в случае интеграции или информационного взаимодействия информационной системы с системами «Электронного Правительства», государственных органов или установки АРМ ГО для оказания электронных услуг государственных*

- Наличие утвержденной технической документации на компоненты информационной системы
- Использование лицензионного ПО и технической поддержки
- Использование ПО по управлению

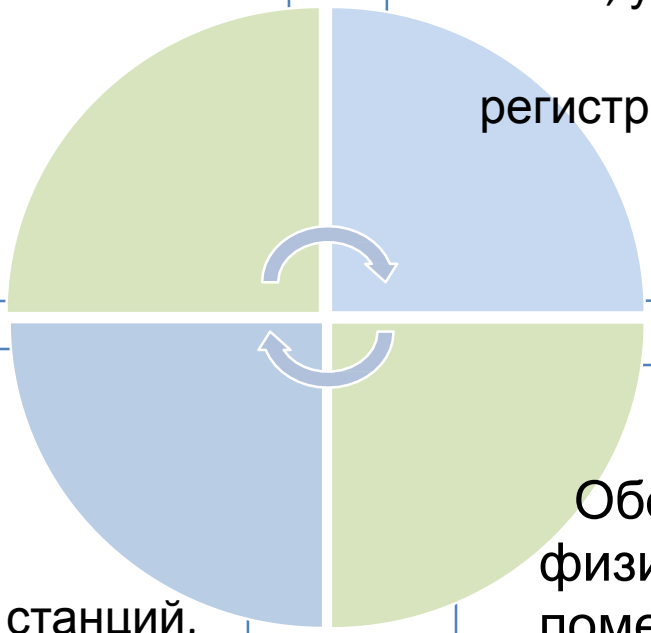
- Использование сканеров для анализа брешей и уязвимостей в ПО
- Использование анализаторов кодов для тестирования программных кодов
- Формирование сценариев тестирования программных кодов информационной системы
- Наличие протоколов тестирования

Информационная система, использующая персональные данные, должна соответствовать требованиям информационной безопасности

Защита инфраструктуры

Обеспечение защиты сетевого оборудования, установка оборудования (FW, IPS), анализаторы трафиика

Обеспечения защиты серверного оборудования и ПО, установка программ обнаружения атак, регистрации всех событий, мониторинга ИБ



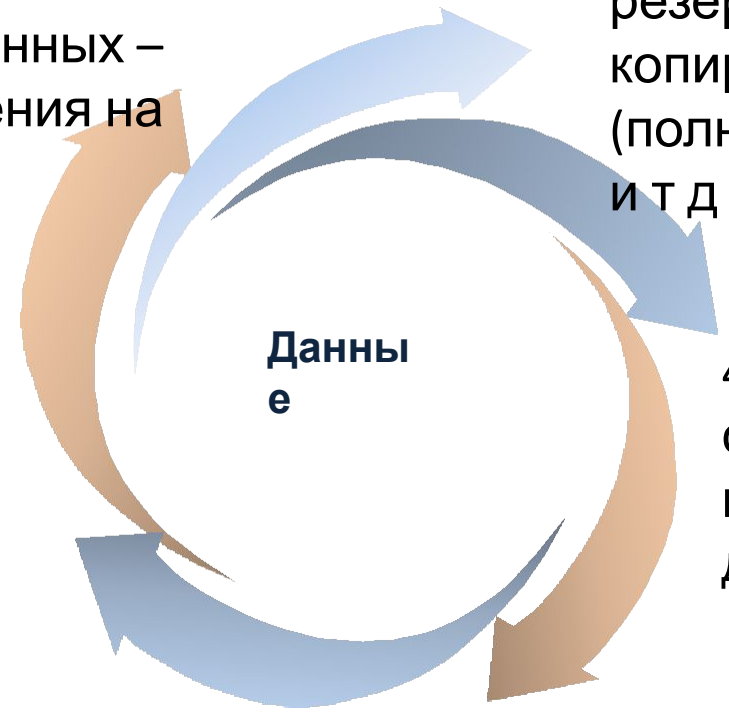
Защита рабочих станций, клиентского ПО, установка DLP систем, ПО фильтрации трафика, использование резервного хранения

Обеспечение физической защиты помещений

Защита данных

1. Обеспечение конфиденциальности персональных данных – наличие разрешения на использование персональной информации

2. Наличие резервного копирования (полного, изменений и т д)



3. Обеспечение защиты персональных данных

4. Наличие системы восстановления данных

5. Анализ комплексной защиты информации

Домашние задание:

Конспект (оформить в виде реферата)

1. **Законы РК ИБ.**
2. **Послание Президента РК.**
3. **Стандарты РК в сфере информационной безопасности.**
4. **Концепция «Киберщит Казахстана».**
5. **Система защиты трансграничного обмена стран ЕС.**