АКТЮБИНСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ
МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ КАЗАХСТАН
ИМ. МАЛКЕДЖАРА БУКЕНБАЕВА

З.З. НҰРЫШ

«ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ»

Учебно-методическое пособие

Актобе, 2025

УДК 343
ББК 67.409
Н 87

Рекомендован к печати Ученым советом Актюбинского юридического института Министерства внутренних дел Республики Казахстан им. М. Букенбаева

Рецензенты:

Сулейманова Г.Ж. - Профессор кафедры уголовного права и криминологии Актюбинского юридического института МВД Республики Казахстан им. М. Букенбаева, кандидат юридических наук.

Садыков М.Т. - Начальник специального отдела «Киберпол» по г. Актобе Департамента полиции Актюбинской области, полковник полиции.

Н87 Нұрыш З.З.

«Основы кибербезопасности» Учебное пособие. – Актобе: // Актюбинский юридический институт МВД Республики Казахстан им. М. Букенбаева, 2025. – 185 с.

Учебное пособие направлено на ознакомление обучающихся с основами цифровой грамотности и кибербезопасности. Включает 10 тем в соответствии с тематическим планом, рассматриваемым по специальности бакалавриата.

Учебное пособие предназначено для курсантов, слушателей, магистрантов и преподавателей учебных заведений системы органов внутренних дел, практических работников.

УДК 343
ББК 67.409
ISBN 9965-608-53-10

СОДЕРЖАНИЕ

1. ПРЕДИСЛОВИЕ

Учебная дисциплина «Основы кибербезопасности» занимает основное место в системе дисциплин высшего юридического образования. Правовое регулирование отношений в киберпространстве в связи с развитием современных информационных и компьютерных технологий растут и их функциональные возможности, что усложняет процесс нахождения на их основе данных правового регулирования основ отношений кибербезопасности. Национальная инфраструктура государства сегодня тесно связана с применением современных компьютерных технологий. Возрастает угроза использования информационных систем государства как способа осуществления компьютерных атак и пиратской деятельности.

Цель изучения дисциплины: «Основы кибербезопасности»: знакомство с Интернет-системами, с которыми в настоящее время обычно связано понятие киберпространства. Все, что происходит в интернете, через веб-сайты, электронную почту, социальные сети, не происходит в определенной стране, за пределами фактического местоположения серверов и пользователей. Киберпространство предоставляет более широкие данные, чем интернет. В этой связи дать общие сведения об основах регулирования правоотношений в киберпространстве.

Изучение наиболее популярных веб-уязвимостей, представленных в сети, изучение основных механизмов использования существующих уязвимостей в расширенных системах, знание того, как исправить уязвимости для снижения риска.

Основными задачами дисциплины: «Основы кибербезопасности» являются формирование общих представлений о безопасности в информационном обществе; опишите общие принципы технологий, применяемых в информационной безопасности; формирование навыков применения правил кибербезопасности во всех сферах деятельности; усвоение знаний, составляющих начало представления об информационной картине мира и информационных процессах; развитие навыков ориентации в информационных потоках.

Образовательная программа регулирует цели, результаты, содержание, условия и технологии реализации образовательного процесса, оценку качества подготовки выпускников данного направления и включает внедрение материалов и соответствующих образовательных технологий, обеспечивающих качество подготовки обучающихся.

Результаты обучения:

Разработка защищенных серверных клиентских веб-приложений и мобильных приложений.

Реализация базовой сетевой связи между устройствами, расчет и применение адресных схем, настройка и установка сетевых устройств.

Демонстрация знаний об архитектуре компьютерных систем, управление операционными системами.

Применение отечественных и зарубежных стандартов по информационной безопасности в организациях.

Применять практические навыки программирования и объяснять общие методологические основы разработки программ, создавать системные программы для драйверов устройств, модулей сопряжения с нестандартным оборудованием и программировать микроконтроллеры.

Разъяснение и понимание законодательной базы Республики Казахстан и других стран, а также процедур стандартизации и сертификации в области информационной безопасности.

Разработка политики информационной безопасности предприятия, применение инструментальных средств управления проектами на различных этапах жизненного цикла проекта, проведение качественной и количественной оценки рисков проектов, определение эффективности проекта с учетом экологической безопасности; критическая оценка и интерпретация информации в области кибербезопасности, экономики и права.

Применение технологий защиты данных в компьютерных системах и сетях.

Проектирование топологии печатных плат, конструктивно-технологических модулей первого уровня с использованием пакетов прикладных программ, анализ микропроцессорных устройств, применение инструментальных средств отладки и тестирования встроенных систем. Системное понимание роли личности и событий в формировании текущей ситуации; возможность критической оценки и размещения действий относительно сложных социальных процессов с учетом исторических факторов. Уметь письменно и устно излагать идеи и суждения по теме информационных технологий, выступать перед аудиторией и отстаивать точку зрения на государственном, английском и межнациональном языках общения.

Пререквизиты: для освоения данной дисциплины необходимы знания и навыки, приобретенные в ходе освоения дисциплин: основы теории государства и права, Уголовное право, уголовно-процессуальное право, Криминалистика.

Постреквизиты: Знания и навыки, приобретенные в ходе освоения данной дисциплины, необходимы для освоения следующих дисциплин: Гражданское процессуальное право, Административное право, Прокурорский надзор, Криминология, Судебная экспертиза.

Политика и процедура дисциплины: курсант обязан регулярно посещать лекционные, семинарские и практические занятия в соответствии с графиком учебных занятий, своевременно готовиться к ним.

Выполняйте письменные и устные задания вовремя, соблюдая требования к этим заданиям. Курсант добросовестно и заранее готовится к занятиям в рамках заданий, предусмотренных для самостоятельной работы с преподавателем и без него. До и после занятий, а также во время лекций и

семинаров необходимо соблюдать требования бакалавриата и преподавателей по поведению.

Посещение занятий обязательно, так как в процессе общения курсанта с преподавателем формируется системность научных знаний, понимание их динамики, способность к самообразованию, позитивное восприятие психолого-педагогических методов и рекомендаций.

Курсанты, пропустившие лекцию, обязаны дополнить оконспект, прочитать рекомендованную литературу и имеющуюся на кафедре лекцию фонда. Или курсанты, получившие неудовлетворительную оценку, обязаны изучить тему по предложенной литературе и сдать ее преподавателю.

При изучении дисциплины курсанты должны соблюдать следующие правила:

- опоздание с занятий без уважительной причины и пропуск занятий без уважительной причины; в случае болезни-справка, в других случаях-пояснительная записка;

- конспектирование нормативно-правовых актов и представленной литературы;

- Своевременная подготовка заданий, указанных в силлабусе; активное участие в учебном процессе.

Для проведения итоговой и текущей успеваемости организуется промежуточный контроль знаний и умений. Оценка определяется с учетом результатов текущего контроля и проставляется в отдельной графе журнала и ведомости.

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Тема №1
«Понятие и содержание киберпространства и кибербезопасности»

Понятие и содержание киберпространства и кибербезопасности. Киберпространство как метафора Интернета. Понятие кибербезопасности в Республике Казахстан. Понятие» киберпространство". Важность феномена глобального обмена информацией. Виртуальные характеристики региона в киберпространстве. Основные функции кибербезопасности. Роль информации в жизни личности, общества и государства. Информационные революции. Понятие глобального информационного пространства. Структура глобального информационного пространства. Виды правового регулирования глобального информационного пространства являются наиболее распространенными кибератаками. Вредоносные программы.

Лекционные занятие

План лекционного занятия:

1. Понятие и содержание киберпространства и кибербезопасности
2. Киберпространство как метафора Интернета
3. Понятие кибербезопасности в Республике Казахстан

Семинарское занятие

План семинарского занятия:

1.Виртуальные характеристики региона в киберпространстве.

2.Основные функции кибербезопасности.

3.Роль информации в жизни личности, общества и государства.

4.Информационные революции. Понятие глобального информационного пространства.

Самостоятельная работа курсанта

1. Задание: подготовить изложение, подготовить эссе, подготовить доклад.

Форма проведения СРК: расширение научного кругозора курсанта через подготовку самостоятельной работы по теме, освоение теоретических методов исследования, развитие самостоятельности мышления курсанта.

2. Методические рекомендации к выполнению: использование данных предложений для лекционных занятий и подготовки к СРК, для получения дополнительных консультаций на кафедре.

3. Для индивидуальной подготовки предлагаются следующие вопросы:

1. Понятие «Киберпространство».

2. Важность феномена глобального обмена информацией. Виртуальные характеристики региона в киберпространстве.

3.Основные функции кибербезопасности.

4.Роль информации в жизни личности, общества и государства.

5. Информационные революции.

6. Понятие глобального информационного пространства.

7. Структура глобального информационного пространства.

8.Виды правового регулирования глобального информационного пространства наиболее распространенные кибератаки. Вредоносные программы.

Тема №2
«Основы обеспечения кибербезопасности и механизмы ее сохранения в условиях глобальной цифровизации»

Аспекты основы кибербезопасности. Теоретические аспекты кибербезопасности, история их развития. Механизм функционирования системы обеспечения кибербезопасности. История возникновения киберпространства. История мировой культуры проблемы освоения человечеством пространства. Цифровая революция. Процессуальные нормы регулирования киберпространства. Требования для регулирования отношений о киберпространстве. Порядок производства по киберпространству. Формирование представления об электронной среде.

Лекционные занятие

План лекционного занятия:

1. Теоретические аспекты кибербезопасности, история их развития
2. Механизм функционирования системы обеспечения кибербезопасности

Семинарское занятие

План семинарского занятия:

1. История возникновения киберпространства.
2. История мировой культуры проблемы освоения человечеством пространства.
3. Цифровая революция.
4. Процессуальные нормы регулирования киберпространства.
5. Требования для регулирования отношений о киберпространстве.

Самостоятельная работа курсанта

1. Задание: решение ситуационных задач

Самостоятельная работа курсанта

1. Задание: подготовить изложение, подготовить эссе, подготовить доклад.

2.Форма проведения СРК: изложение в письменной форме сути поставленной проблемы, самостоятельный анализ данной проблемы с использованием концепций и аналитических средств соответствующей дисциплины, подведение итогов, обобщающих авторскую позицию по поставленной проблеме.

Методические рекомендации к выполнению: использование данных предложений для лекционных занятий и подготовки к СРК, для получения дополнительных консультаций на кафедре.

Для индивидуальной подготовки предлагаются следующие вопросы:

1. Информационная инфраструктура
2. Международные договоры о киберпространстве.

3.Условия использования информационных и коммуникационных технологий как средства разрешения межгосударственных конфликтов.

4.Сотрудничество о киберпространстве.

Тема №3
«Правовые вопросы обеспечения безопасности в киберпространстве. Исторический анализ»

Проблемы кибербезопасности в защите информационного пространства. Правовые вопросы обеспечения безопасности в киберпространстве. Обеспечение безопасности в киберпространстве в сфере государственной политики. Правовые вопросы обеспечения безопасности в киберпространстве. Исторический анализ. Проблемы кибербезопасности. Экосистема кибербезопасности. Проблемы обеспечения кибербезопасности. Информационная безопасность (кибербезопасность) в сфере информатизации состояние защищенности электронных информационных ресурсов, информационных систем и информационно – коммуникационной инфраструктуры от внешних и внутренних угроз. Типы угроз кибербезопасности. Электронная цифровая подпись использование цифровой подписи.

Лекционные занятие

План лекционного занятия:

1.Проблемы кибербезопасности в защите информационного пространства.

2. Правовые вопросы обеспечения безопасности в киберпространстве.

3.Обеспечение безопасности в киберпространстве в сфере государственной политики.

Семинарское занятие

План семинарского занятия:

1. Правовые вопросы обеспечения безопасности в киберпространстве. Исторический анализ.

2. Проблемы кибербезопасности.

3. Экосистема кибербезопасности.

4. Проблемы обеспечения кибербезопасности.

Самостоятельная работа курсанта

1.Задание: подготовить презентацию по теме (слайд)

Форма проведения СРК: разъяснение, дискуссия, собеседование

Самостоятельная работа курсанта

1. Задание: составить сводную (обобщающую) таблицу

Форма проведения СРК: освоение отношений между понятиями или отдельными разделами темы путем составления таблицы

1. Методические рекомендации к выполнению: использование данных предложений для лекционных занятий и подготовки к СРК, для получения дополнительных консультаций на кафедре.

2. Для индивидуальной подготовки предлагаются следующие вопросы:

1.Проблемы кибербезопасности в защите информационного пространства.

2. Правовые вопросы обеспечения безопасности в киберпространстве.

3.Обеспечение безопасности в киберпространстве в сфере государственной политики.

4.Правовые вопросы обеспечения безопасности в киберпространстве. Исторический анализ.

5. Проблемы кибербезопасности.

6.Экосистема кибербезопасности. Проблемы обеспечения кибербезопасности.

7.Информационная безопасность (кибербезопасность) в сфере информатизации состояние защищенности электронных информационных ресурсов, информационных систем и информационно – коммуникационной инфраструктуры от внешних и внутренних угроз.

8. Типы угроз кибербезопасности. Электронная цифровая подпись использование цифровой подписи.

Тема №4
«Соблюдение норм кибергигиены. Противодействие киберпреступности»

Что такое Кибергигиена? Профилактика кибергигиены. Защита от кибератак. Настройка функций автоматического обновления программного обеспечения.

Защита от атак социальной инженерии. Кибергигиена. Соблюдение норм кибергигиены. Совершенствование системы кибербезопасности. Противодействие киберпреступности. Одна из ключевых частей программы «кибербезопасность» - это обучение специалистов в области кибербезопасности и важность информационной безопасности для общественности. Фишинговые сайты. Киберпреступность.

Лекционные занятие

План лекционного занятия:

1. Кибергигиена. Соблюдение норм кибергигиены.
2. Совершенствование системы кибербезопасности.
3. Противодействие киберпреступности

Семинарское занятие

План семинарского занятия:

1. Кибергигиена. Соблюдение норм кибергигиены.
2. Совершенствование системы кибербезопасности.

Самостоятельная работа курсанта

1. Задание: подготовить изложение по теме

2. Форма проведения СРК: подготовка изложения по предлагаемым темам.

1. Совершенствование системы кибербезопасности.

1.Противодействие киберпреступности.

2.Одной из основных частей программы» кибербезопасность " является обучение специалистов в области кибербезопасности и важность информационной безопасности для общественности.

3.Фишинговые сайты.

4. Киберпреступность.

Методические рекомендации к выполнению: использование данных предложений для лекционных занятий и подготовки к СИП, для получения дополнительных консультаций на кафедре.

Для индивидуальной подготовки предлагаются следующие вопросы:

1. Что такое нарушение работы информационной системы или информационно-коммуникационной сети?

2. Незаконное присвоение информации?

3. Оказание услуг для размещения интернет-ресурсов, преследующих незаконные цели?

Тема №5
«Пути повышения кибербезопасности в Республике Казахстан»

Современные элементы информационно-коммуникационной инфраструктуры. Возможности применения современных информационных технологий во всех сферах государственной и общественной деятельности.

Использование информационных технологий, телекоммуникационных систем и соответствующих технических средств с высокой тенденцией к современному общественному развитию. Совершенствование информационного законодательства. Законодательные различия понятий «Кибербезопасность» и «Информационная безопасность». Законодательство в области кибербезопасности и информационных коммуникаций в Республике Казахстан. Определение термина «кибербезопасность» в Концепции кибербезопасности Казахстана и понятия «информационная безопасность в сфере информатизации» в Закон Республики Казахстан «Об информатизации».

Лекционные занятие

План лекционного занятия:

1. Законодательные различия понятий «Кибербезопасность» и «Информационная безопасность»
2. Законодательство в области кибербезопасности и информационных коммуникаций в Республике Казахстан

Семинарское занятие

План семинарского занятия:

1. Совершенствование информационного законодательства.
2. Законодательные различия понятий «Кибербезопасность» и «Информационная безопасность».

Самостоятельная работа курсанта

1. Задание: выполнить ситуационные задания
2. Форма проведения СРК: выполнение заданий

Ситуационные задачи:

Задание № 1

Инструкция. Выберите несколько предложенных вариантов правильных ответов.

Задание. Разработчик игры "Stoon" потратил на ее создание пять лет. Когда «камень» сдавали в аренду, сын Лени хотел купить эту игру. Придя в магазин, он обнаружил, что стоимость высока, поэтому решил пойти в Интернет за помощью. Перейдя по первой ссылке в сети, Леня увидел надпись "игра" Stoon "бесплатна и ее можно скачать по ссылке ниже". Выберите вариант, который вы порекомендуете Лене, из вариантов ниже.

Загрузите игру с этого сайта, так как она бесплатна.

Попросите у родителей деньги и сделайте покупки в магазине.

Продолжить поиск в интернете с возможностью покупки игры со скидкой.

Правильные ответы: Б и В.

Самостоятельная работа курсанта

1. Задание: выполнить тестовые задания

2. Форма проведения СРК: письменный ответ

Методические рекомендации к выполнению: использование данных предложений для лекционных занятий и подготовки к СРК, для получения дополнительных консультаций на кафедре.

Для индивидуальной подготовки предлагаются следующие вопросы:

1.Законодательные различия понятий» Информационная безопасность".

2.Законодательство в области кибербезопасности и информационных коммуникаций в Республике Казахстан.

3.Дайте определение термину «кибербезопасность» в Концепции кибербезопасности Казахстана и понятию «информационная безопасность в сфере информатизации» в Законе Республики Казахстан «Об информатизации».

Тема №6
«Законодательство в области кибербезопасности и информационных коммуникаций»

Обеспечение кибербезопасности. Обеспечение кибербезопасности. удобство и преимущества цифрового мира. Цифровизация экономики. Риски, связанные с цифровизацией экономики.

Обеспечение кибербезопасности. Внедрение цифровых технологий. Использование новых технологий и преимуществ цифровой грамотности. Анализ результатов использования цифровых технологий. Анализ существующих механизмов использования и внедрения кибербезопасности. Экономические факторы. Социокультурные факторы. Технологические факторы. Политические факторы. Экономические факторы. Социокультурные факторы. Технологические факторы.

Лекционные занятие

План лекционного занятия:

1. Анализ результатов использования цифровых технологий.
2. Анализ существующих механизмов использования и внедрения кибербезопасности

Семинарское занятие

План семинарского занятия:

1.Обеспечение кибербезопасности.
2. Внедрение цифровых технологий.
3.Использование новых технологий и преимуществ цифровой грамотности.

Самостоятельная работа курсанта с преподавателем

1. Задание: выполнить ситуационные задания
2. Форма проведения СРК: выполнение ситуационных заданий

Ситуационные задачи:

Задачи №1

Инструкция. Прочитайте описание ситуации и дайте исчерпывающий ответ на поставленные вопросы.

Задание. Когда мама Кати пришла на работу, она обнаружила, что забыла свой мобильный телефон дома. С рабочего телефона он попросил Катю привести его на работу. Закончив разговор, Катя услышала, как в соседней комнате на мобильный телефон ее матери пришло sms-сообщение. Поскольку у Кати и ее матери были доверительные отношения, девушка прочитала полученное SMS-сообщение. Катя заметила, что сообщение пришло от неизвестного отправителя. Он содержит следующий текст:

"Добрый день! По паспортным данным найдены страховые выплаты в размере 47 рублей. Подробнее на сайте: http://snils-gost.online». Девушка, не задумываясь, перешла на ссылку. В открывшемся окне браузера отсутствовала информация о паспортных данных матери, и Катя закрыла его. Через несколько минут на мобильный телефон пришло SMS-сообщение от оператора сотовой связи:"Ваш баланс меньше 5 рублей". Подозревая, что потеря средств связана с переходом по ссылке из СМС-сообщения, Катя испугалась и бросилась к матери на работу.

Какие ошибки совершила Катя?

Вопрос в том, какие последствия могут возникнуть от действий Кати? Обоснуйте свой ответ.

Предложите этим детям описать симптомы SMS-мошенничества и правила поведения при встрече с ними.

Правильные ответы:

а) прочитал сообщение, которое ему не прислали, перешел по подозрительной ссылке.

б) перейти по ссылке 1) списать деньги со счета, 2) на телефон, который перестает нормально работать и загружает все персональные данные, могут загрузиться вирусы, 3) при подключении телефона к компьютеру данное устройство также может быть заражено.

в) СМС-признаки мошенничества: номер неизвестного отправителя; номер очень короткий; сообщение содержит информацию о выигрыше, для получения которой необходимо пройти по указанной ссылке; требование обратного звонка; просьба о помощи в связи с переводом денег. Правила поведения: никогда не перезванивайте и не переводите деньги; удалите SMS-сообщение; перезвоните оператору сотовой связи, чтобы решить" проблему"; установите антивирусную программу на свой телефон.

2. Форма проведения СРК: выполнение тестовых заданий

Методические рекомендации к выполнению: использование данных предложений для лекционных занятий и подготовки к СРК, для получения дополнительных консультаций на кафедре.

1. Для индивидуальной подготовки предлагаются следующие вопросы:

1. Обеспечение кибербезопасности.

2. Обеспечение кибербезопасности. удобство и преимущества цифрового мира.

3. Цифровизация экономики.

4. Риски, связанные с цифровизацией экономики.

5. Обеспечение кибербезопасности.

6. Внедрение цифровых технологий.

7. Использование новых технологий и преимуществ цифровой грамотности.

8. Анализ результатов использования цифровых технологий.

9.Анализ существующих механизмов использования и внедрения кибербезопасности. Экономические факторы.

10. Социокультурные факторы.
11. Технологические факторы.
12. Политические факторы.
13. Экономические факторы.
14. Социокультурные факторы.
15. Технологические факторы.

Тема №7
«Анализ обеспечения кибербезопасности в Республике Казахстан»

Проблемные аспекты реализации программы "Цифровой Казахстан". Государственный и частный секторы являются потенциальными киберугрозами в цифровом пространстве республики. Политика обеспечения кибербезопасности в Республике Казахстан. Основные проблемы международного опыта и кибербезопасности. Надзор и поддержка национальной кибербезопасности Казахстана. Расширение преимуществ Казахстана в области кибербезопасности. Национальная стратегия кибербезопасности. Развитие электронного правительства. Развитие цифровой культуры. Развитие цифрового здравоохранения. Развитие цифровой инфраструктуры. Совершенствование системы управления обеспечением кибербезопасности в Республике Казахстан. Совершенствование рекомендаций по обеспечению кибербезопасности в Республике Казахстан.

Лекционные занятие

План лекционного занятия:

1.Совершенствование системы управления обеспечением кибербезопасности в Республике Казахстан

2. Совершенствование рекомендаций по обеспечению кибербезопасности в Республике Казахстан

Семинарское занятие

План семинарского занятия:

1. Проблемные аспекты реализации программы «Цифровой Казахстан».
2. Политика обеспечения кибербезопасности в Республике Казахстан. Основные проблемы международного опыта и кибербезопасности.

Самостоятельная работа курсанта

Задание:

Вам пришло письмо на электронную почту следующего содержания:" чтобы подтвердить, что вы являетесь пользователем "Вконтакте", перейдите по этой ссылке https://vvk.com/id47073790". щелкнуть ссылку и почему? Обоснуйте свой ответ.

Правильный ответ. Перейти по ссылке невозможно. Этот адрес не является официальным адресом сайта "Вконтакте", так как в адресе есть дополнительная буква v — vvk.com, мошенник может получить доступ к вашим личным данным, если вы введете логин и пароль при входе по этой ссылке.

Форма проведения СРК: развитие навыков и умений грамотного изложения теории и практических вопросов в письменной форме в виде конспекта.

Методические рекомендации к выполнению: использование данных предложений для лекционных занятий и подготовки к СРК, для получения дополнительных консультаций на кафедре.

Для индивидуальной подготовки предлагаются следующие вопросы:

1. Расширение преимуществ Казахстана в области кибербезопасности.
2. Национальная стратегия кибербезопасности.
3. Развитие электронного правительства.
4. Развитие цифровой культуры.
5. Развитие цифрового здравоохранения. Развитие цифровой инфраструктуры.
6. Совершенствование системы управления обеспечением кибербезопасности в Республике Казахстан.
7. Совершенствование рекомендаций по обеспечению кибербезопасности в Республике Казахстан.

Тема №8
«Основные положения о киберпреступности. Виртуальное мошенничество и кибербуллинг»

Мошенничество в области компьютерной информации. Досудебное расследование в области информационных технологий борьба с преступлениями, совершаемыми с использованием компьютерных систем и сетей. Противодействие киберпреступности. Расследование уголовных правонарушений в сфере информатизации и связи. Уголовные правонарушения в сфере информатизации и связи. Соблюдение принципов законности и справедливости в процессе расследования. Кибербуллинг. Предотвращение кибербуллинга. Формы кибербуллинга. Кибератака. Международный опыт. Киберкультура. Кибербуллинг и кибербезопасность.

Лекционные занятие

План лекционного занятия:

1. Виртуальное мошенничество. Мошенничество в киберпространстве.
2. Кибербуллинг. Предотвращение кибербуллинга.

Семинарское занятие

План семинарского занятия::

1.Мошенничество в области компьютерной информации.

2.Досудебное расследование в области информационных технологий борьба с преступлениями, совершаемыми с использованием компьютерных систем и сетей.

3.Противодействие киберпреступности.

4.Расследование уголовных правонарушений в сфере информатизации и связи.

Самостоятельная работа курсанта

1. Задание: подготовить эссе по теме
2. Форма проведения СРК: разъяснение, дискуссия, собеседование

Самостоятельная работа курсанта

1. Задание: подготовить изложение, эссе по теме, подготовить доклад.

2. Форма проведения СРК: расширение научного кругозора по теме, Освоение теоретических методов исследования, развитие самостоятельности мышления курсанта.

Методические рекомендации к выполнению: использование данных предложений для лекционных занятий и подготовки к СРК, для получения дополнительных консультаций на кафедре.

Задачи

Инструкция. Прочитайте описание ситуации и дайте исчерпывающий ответ на поставленные вопросы.

Задание. Прогуливаясь по торговому центру, Таня увидела платье, которое ей нравилось, но оно было дорогим. Девушка решила проверить, сколько стоит это платье в интернет-магазине. Не раздумывая, он подключился к одной из открытых сетей "FreeWiFi", которую нашел. Зайдя на сайт Интернет-магазина, девушка нашла именно такое платье, но оно стоит в 3 раза дешевле. Обрадовавшись, Таня оформила онлайн-покупку, введя номер банковской карты и трехзначный код на обратной стороне карты. После этого она зашла в социальные сети и поделилась своей радостной новостью со своей девушкой.

1. Какие ошибки совершила Таня?

2. Какие негативные последствия может иметь совершенное им действие? Обоснуйте свой ответ.

3.Сформулируйте правила, которыми следует руководствоваться при использовании общедоступной сети Wi-Fi.

Правильные ответы.

1.Подключившись к общедоступной сети Wi – Fi, Таня предоставила конфиденциальные данные: ввела номер и код с банковской карты, зашла в социальную сеть, ввела логин и пароль.

2. Негативные последствия совершенного действия: используя введенный Таней логин и пароль, злоумышленники могут "взломать" ее страницу в соцсети, таким образом, узнать личную информацию от имени Тани, попросить денег у "друзей", шантажировать саму Таню и т.д. Кроме того,так как при покупке Таня ввела трехзначный код с карты, теперь мошенники могут использовать его карту, оплачивая его покупки в интернете.

3.Правила: не доверять сетям с подозрительными именами (FreeInternet или FreeWiFi), не совершать онлайн-покупки и банковские переводы в общедоступных сетях, не отправлять конфиденциальную информацию, не вводить логины и пароли с разных сайтов.

Тема №9
«Концепция кибербезопасности Республики Казахстан. Цели, задачи, ожидаемые результаты и период реализации Концепции кибербезопасности»

Понятие технологического лидерства в информационном пространстве. Военное лидерство в кибербезопасности. Дайте определение «кибервойны» информационная война: проблемы и решения. Понятие кибербезопасности РК. Киберзащита глобальной сети. Проблемы кибербезопасности. Основные угрозы кибербезопасности. Цели и задачи кибербезопасности РК. Ожидаемые результаты концепции кибербезопасности. Этапы реализации Концепции кибербезопасности. Анонимность в киберпространстве. Основные принципы в концепции киберпространства. Международные подходы к безопасности в сфере киберпространства. Подходы государств к решению проблем. Кибер-стратегия государств.

Лекционные занятие

План лекционного занятия:

1.Концепция цифровой трансформации, развития сферы информационно-коммуникационных технологий и кибербезопасности.

2.Цели, задачи, ожидаемые результаты и период реализации Концепции кибербезопасности.

Семинарское занятие

План семинарского занятия:

1.Киберзащита глобальной сети.

2. Проблемы кибербезопасности. Основные угрозы кибербезопасности.

3.Цели и задачи кибербезопасности РК. Ожидаемые результаты концепции кибербезопасности.

4. Этапы реализации Концепции кибербезопасности.

5.Анонимность в киберпространстве.

6.Основные принципы в концепции киберпространства.

Самостоятельная работа курсанта

1. Задание: подготовить схему по теме

2. Форма проведения СРК: разъяснение, дискуссия, собеседование

Самостоятельная работа курсанта

1. Задание: подготовить изложение по теме, подготовить доклад, подготовить эссе.

2.Форма проведения СРК: выполнение задания способствует расширению научного кругозора курсанта, освоению теоретических методов исследования, развитию самостоятельности мышления курсанта.

Методические рекомендации к выполнению: использование данных предложений для лекционных занятий и подготовки к СРК, для получения дополнительных консультаций на кафедре.

Задание. Инструкция. Прочитайте описание ситуации и дайте исчерпывающий ответ на поставленные вопросы.

Света (16 лет) рассталась со своим молодым человеком и очень переживала по этому поводу. Чтобы понять причины развода, девушка начала искать в интернете информацию об отношениях между людьми противоположного пола. На одном из световых форумов я прочитал похожую историю. Он написал автору сообщение, тем самым начав переписку с незнакомцем. Виртуальная собеседница рассказала, что ее зовут Настя, и она живет в том же городе. Они вместе обсуждали, что произошло, делились своими чувствами и переживаниями. В одном из сообщений Настя написала, что для того, чтобы забыть несчастную любовь, нужно найти хобби, хобби. Настя предложила Светке встретиться и вместе пойти в танцевальную студию.

1. Стоит ли договариваться о встрече с Настей? Обоснуйте свой ответ.

2. Какие могут быть негативные последствия встречи Света и ее виртуального собеседника?

3. Какие способы освещения могут защитить себя?

Правильные ответы.

1.Света не должна соглашаться на встречу, потому что не может быть уверена, кто на самом деле виртуальный собеседник.

2.Возможные негативные последствия: участвует в религиозных или экстремистских организациях, становится жертвой конкретного преступника.

3.Собираясь на свидание, Света обязательно должна сообщить любимому человеку, с кем встретиться и куда он ушел, когда вышел на связь. Назначьте встречу в людном и знакомом месте.

Тема №10
«Международный опыт. Модели обеспечения кибербезопасности развитых зарубежных стран на современном этапе»

«Международный опыт». Модели обеспечения кибербезопасности развитых зарубежных стран на современном этапе. Информационные сети, составляющие основу киберпространства. Нормы поведения государств в киберпространстве. Основные принципы в концепции киберпространства. Международные подходы к безопасности в сфере киберпространства. Подходы государств к решению проблем. Национальная стратегия кибербезопасности и Общенациональный план по ее внедрению. Государственное управление в области обеспечения кибербезопасности. Цифровая трансформация. Развитие цифровой инфраструктуры «Киберщит Казахстана». Международный опыт и сотрудничество в области кибербезопасности и информационной безопасности.

Лекционные занятие

План лекционного занятия:

1. Международный опыт
2. Модели обеспечения кибербезопасности развитых зарубежных стран на современном этапе.

Семинарское занятие

План семинарского занятия:

1. Государственное управление в области обеспечения кибербезопасности.
2. Цифровая трансформация.
3. Развитие цифровой инфраструктуры "Киберщит Казахстана".
4. Международный опыт и сотрудничество в области кибербезопасности и информационной безопасности.

Самостоятельная работа курсанта

1. Задание: выполнить доклад по теме
2. Форма проведения СРК: выбор темы из предложенных тем

1. «Международный опыт».
2. Модели обеспечения кибербезопасности развитых зарубежных стран на современном этапе.
3. Информационные сети, составляющие основу киберпространства.
4. Нормы поведения государств в киберпространстве.
5. Основные принципы в концепции киберпространства.
6. Развитие цифровой инфраструктуры "Киберщит Казахстана".
7. Международный опыт и сотрудничество в области кибербезопасности и информационной безопасности.

Методические рекомендации к выполнению: использование данных

предложений для лекционных занятий и подготовки к СИП, для получения дополнительных консультаций на кафедре.

Для индивидуальной подготовки предлагаются следующие вопросы:

1. Международные подходы к безопасности в сфере киберпространства.

2. Подходы государств к решению проблем.

3. «Национальная стратегия кибербезопасности» и «Общенациональный план по ее внедрению».

4.Государственное управление в области обеспечения кибербезопасности. Цифровая трансформация.

3. ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ОЦЕНКИ УЧЕБНЫХ ДОСТИЖЕНИЙ ОБУЧАЮЩИХСЯ:

1. Что такое кибербезопасность?
2. Назовите элементы кибербезопасности.
3. Перечислите наиболее распространенные кибератаки.
4. Определите информационную безопасность.
5. Перечислите обязанности специалиста по информационной безопасности.
6. Что такое Криптография?
7. Какие существуют виды криптографии и для чего они используются?
8. Что такое электронная подпись и чем она отличается от хештега?
9. Что изменится с вступлением в силу нового указа?
10. Кто должен создавать центры кибербезопасности?
11. Нужно ли что-то менять тем компаниям, у которых все чисто с информационной безопасностью?
12. Есть ли возможность передать кибербезопасность на аутсорсинг?
13. Чем Информационная безопасность отличается от кибербезопасности?
14. Понятие «киберпространство».
15. Важность феномена глобального обмена информацией. Виртуальные характеристики региона в киберпространстве.
16. Основные функции кибербезопасности.
17. Роль информации в жизни личности, общества и государства.
18. Информационные революции.
19. Понятие глобального информационного пространства.
20. Структура глобального информационного пространства.
21. Виды правового регулирования глобального информационного пространства наиболее распространенные кибератаки. Вредоносные программы
22. Информационная инфраструктура
23. Международные договоры о киберпространстве.
24. Условия использования информационных и коммуникационных технологий как средства разрешения межгосударственных конфликтов.
25. Сотрудничество в киберпространстве.
26. Правовые вопросы обеспечения безопасности в киберпространстве. Исторический анализ.
27. Проблемы кибербезопасности.
28. Экосистема кибербезопасности.
29. Проблемы обеспечения кибербезопасности.
30. Проблемы кибербезопасности в защите информационного пространства.
31. Правовые вопросы обеспечения безопасности в киберпространстве.

32. Обеспечение безопасности в киберпространстве в сфере государственной политики.

33. Правовые вопросы обеспечения безопасности в киберпространстве. Исторический анализ.

34. Проблемы кибербезопасности.

35. Экосистема кибербезопасности.

36. Проблемы обеспечения кибербезопасности.

37. Информационная безопасность (кибербезопасность) в сфере информатизации состояние защищенности электронных информационных ресурсов, информационных систем и информационно – коммуникационной инфраструктуры от внешних и внутренних угроз.

38. Виды угроз кибербезопасности.

39. Использование электронной цифровой подписи с использованием цифровой подписи.

40. Что такое нарушение работы информационной системы или информационно-коммуникационной сети?

41. Незаконное присвоение информации?

42. Оказание услуг для размещения интернет-ресурсов, преследующих незаконные цели?

43. Законодательные различия понятий "Информационная безопасность".

44. Законодательство в области кибербезопасности и информационных коммуникаций в Республике Казахстан.

45. Дайте определение термину «кибербезопасность» и «информационная безопасность в сфере информатизации».

46. Обеспечение кибербезопасности.

47. Обеспечение кибербезопасности.

48. Удобство и преимущества цифрового мира.

49. Цифровизация экономики.

50. Риски, связанные с цифровизацией экономики.

51. Обеспечение кибербезопасности.

52. Внедрение цифровых технологий.

53. Использование новых технологий и преимуществ цифровой грамотности.

54. Анализ результатов использования цифровых технологий.

55. Анализ существующих механизмов использования и внедрения кибербезопасности.

56. Экономические факторы.

57. Социокультурные факторы.

58. Технологические факторы.

59. Политические факторы.

60. Экономические факторы.

61. Социокультурные факторы.

62. Технологические факторы.

63. Расширение преимуществ Казахстана в области кибербезопасности.
64. Национальная стратегия кибербезопасности.
65. Развитие электронного правительства.
66. Развитие цифровой культуры.
67. Развитие цифрового здравоохранения.
68. Развитие цифровой инфраструктуры.
69. Совершенствование системы управления обеспечением кибербезопасности в Республике Казахстан.
70. Совершенствование рекомендаций по обеспечению кибербезопасности в Республике Казахстан.
71. Мошенничество в области компьютерной информации.
72. Досудебное расследование в области информационных технологий борьба с преступлениями, совершаемыми с использованием компьютерных систем и сетей.
73. Противодействие киберпреступности.
74. Расследование уголовных правонарушений в сфере информатизации и связи.
75. Киберзащита глобальной сети.
76. Проблемы кибербезопасности.
77. Основные угрозы кибербезопасности.
78. Цели и задачи кибербезопасности РК.
79. Ожидаемые результаты Концепции кибербезопасности.
80. Этапы реализации Концепции кибербезопасности.
81. Анонимность в киберпространстве.
82. Основные принципы в концепции киберпространства.
83. Международный опыт.
84. Модели обеспечения кибербезопасности развитых зарубежных стран на современном этапе.
85. Информационные сети, составляющие основу киберпространства.
86. Нормы поведения государств в киберпространстве.
87. Что такое Криптография?
88. Основные принципы в концепции киберпространства.
89. Развитие цифровой инфраструктуры "Киберщит Казахстана".
90. Международный опыт и сотрудничество в области кибербезопасности и информационной безопасности.
91. Что такое Брандмауэр?
92. Что такое утечка данных?
93. Объясните атаку грубой силой. Как этого избежать?
94. Что такое сканирование портов?
95. Что такое черные хакеры?
96. Что такое белые хакеры?
97. Что такое взлом?
98. Кто такие хакеры?
99. Что такое прослушивание сети?

100. Объясните уязвимости сетевой безопасности.

101. Основные концептуальные положения системы защиты информации

102. Действия, приводящие к незаконному усвоению конфиденциальной информации.

103. Общие положения способов защиты информации.

104. Противодействие незаконному подключению к сетям связи.

105. Направления взаимодействия с зарубежными партнерами в области информационной безопасности.

106. Научно-техническое сотрудничество. Технологический обмен и его регулирование.

107. Порядок защиты конфиденциальной информации при работе с иностранными партнерами.

108. Основные понятия и правила защиты информации.

109. Основные угрозы информационной безопасности при подключении к интернету.

110. Информация, информационные правоотношения. Определение безопасности и ее компонент.

111. Система защиты информации. Структура системы безопасности предприятия. Структура угроз информационной безопасности.

112. Объекты защиты на персональных компьютерах и компьютерных системах.

113. Национальные интересы РК в информационной сфере и их обеспечение.

114. Организационные методы защиты информационных процессов.

115. Концептуальные основы защиты информации.

116. Концептуальные основы построения защиты информационных процессов в компьютерных системах от несанкционированного доступа.

117. Выделение средств защиты информационных процессов в компьютерных системах.

118. Ограничение доступа к документам, ресурсам ПК и сети.

119. Защита электронных документов.

120. Какие правовые проблемы связаны с расследованием киберпреступности и предупреждением киберпреступности.

121.Какие оперативные вопросы связаны с расследованием киберпреступлений и предупреждением киберпреступности.

122.Дайте определение киберпреступности. Вот как делается эта киберпреступность.

123. Последствия отсутствия национальных законов о киберпреступности.

124. Киберпреступность нарушение территориального суверенитета.

125.Принципы, входящие в Национальную стратегию кибербезопасности.

126. Обеспечение соблюдения национальных законов О защите данных.

127.Требования по обеспечению безопасности данных.

128.Правонарушения в отношении авторских прав и товарных знаков, совершаемые посредством кибертехнологий.

129. Концептуализация организованной преступности и ее участники.

130.Информационная война, дезинформация и мошенничество.

4. СБОРНИК СИТУАЦИОННЫХ ЗАДАЧ

Задачи №1

Инструкция. Выберите несколько предложенных вариантов правильных ответов.

Задание. Разработчик игры "Stoon" потратил на ее создание пять лет. Когда «камень» сдавали в аренду, сын Лени хотел купить эту игру. Придя в магазин, он обнаружил, что стоимость высока, поэтому решил пойти в Интернет за помощью. Перейдя по первой ссылке в сети, Леня увидел надпись "игра" Stoon "бесплатна и ее можно скачать по ссылке ниже". Выберите вариант, который вы порекомендуете Лене, из вариантов ниже.

Загрузите игру с этого сайта, так как она бесплатна.

Попросите у родителей деньги и сделайте покупки в магазине.

Продолжить поиск в интернете с возможностью покупки игры со скидкой.

Правильные ответы: Б и В.

Задачи №2

Инструкция. Прочитайте описание ситуации и дайте исчерпывающий ответ на поставленные вопросы.

Задание. Когда мама Кати пришла на работу, она обнаружила, что забыла свой мобильный телефон дома. С рабочего телефона он попросил Катю привести его на работу. Закончив разговор, Катя услышала, как в соседней комнате на мобильный телефон ее матери пришло sms-сообщение. Поскольку у Кати и ее матери были доверительные отношения, девушка прочитала полученное SMS-сообщение. Катя заметила, что сообщение пришло от неизвестного отправителя. Он содержит следующий текст: "Добрый день! По паспортным данным найдены страховые выплаты в размере 47 рублей. Подробнее на сайте: http://snils-gost.online». Девушка, не задумываясь, перешла на ссылку. В открывшемся окне браузера отсутствовала информация о паспортных данных матери, и Катя закрыла его. Через несколько минут на мобильный телефон пришло SMS-сообщение от оператора сотовой связи:"Ваш баланс меньше 5 рублей". Подозревая, что потеря средств связана с переходом по ссылке из СМС-сообщения, Катя испугалась и бросилась к матери на работу.

Какие ошибки совершила Катя?

Вопрос в том, какие последствия могут возникнуть от действий Кати? Обоснуйте свой ответ.

Предложите этим детям описать симптомы SMS-мошенничества и правила поведения при встрече с ними.

Правильные ответы:

а) прочитал сообщение, которое ему не прислали, перешел по подозрительной ссылке.

б) перейти по ссылке 1) списать деньги со счета, 2) на телефон, который

перестает нормально работать и загружает все персональные данные, могут загрузиться вирусы, 3) при подключении телефона к компьютеру данное устройство также может быть заражено.

в) СМС-признаки мошенничества: номер неизвестного отправителя; номер очень короткий; сообщение содержит информацию о выигрыше, для получения которой необходимо пройти по указанной ссылке; требование обратного звонка; просьба о помощи в связи с переводом денег. Правила поведения: никогда не перезванивайте и не переводите деньги; удалите SMS-сообщение; перезвоните оператору сотовой связи, чтобы решить "проблему"; установите антивирусную программу на свой телефон.

Задачи №3

Задание:

Вам пришло письмо на электронную почту следующего содержания:" чтобы подтвердить, что вы являетесь пользователем "Вконтакте", перейдите по этой ссылке https://vvk.com/id47073790". щелкнуть ссылку и почему? Обоснуйте свой ответ.

Правильный ответ. Перейти по ссылке невозможно. Этот адрес не является официальным адресом сайта "Вконтакте", так как в адресе есть дополнительная буква v — vvk.com, мошенник может получить доступ к вашим личным данным, если вы введете логин и пароль при входе по этой ссылке.

Задачи №4

Инструкция. Прочитайте описание ситуации и дайте исчерпывающий ответ на поставленные вопросы.

Задание. Прогуливаясь по торговому центру, Таня увидела платье, которое ей нравилось, но оно было дорогим. Девушка решила проверить, сколько стоит это платье в интернет-магазине. Не раздумывая, он подключился к одной из открытых сетей "FreeWiFi", которую нашел. Зайдя на сайт Интернет-магазина, девушка нашла именно такое платье, но оно стоит в 3 раза дешевле. Обрадовавшись, Таня оформила онлайн-покупку, введя номер банковской карты и трехзначный код на обратной стороне карты. После этого она зашла в социальные сети и поделилась своей радостной новостью со своей девушкой.

1. Какие ошибки совершила Таня?

2. Какие негативные последствия может иметь совершенное им действие? Обоснуйте свой ответ.

3.Сформулируйте правила, которыми следует руководствоваться при использовании общедоступной сети Wi-Fi.

Правильные ответы.

1.Подключившись к общедоступной сети Wi – Fi, Таня предоставила конфиденциальные данные: ввела номер и код с банковской карты, зашла в социальную сеть, ввела логин и пароль.

2. Негативные последствия совершенного действия: используя введенный Таней логин и пароль, злоумышленники могут "взломать" ее страницу в соцсети, таким образом, узнать личную информацию от имени Тани, попросить денег у "друзей", шантажировать саму Таню и т.д. Кроме того,так как при покупке Таня ввела трехзначный код с карты, теперь мошенники могут использовать его карту, оплачивая его покупки в интернете.

3.Правила: не доверять сетям с подозрительными именами (FreeInternet или FreeWiFi), не совершать онлайн-покупки и банковские переводы в общедоступных сетях, не отправлять конфиденциальную информацию, не вводить логины и пароли с разных сайтов.

Задачи №5

Инструкция. Прочитайте описание ситуации и дайте исчерпывающий ответ на поставленные вопросы.

Света (16 лет) рассталась со своим молодым человеком и очень переживала по этому поводу. Чтобы понять причины развода, девушка начала искать в интернете информацию об отношениях между людьми противоположного пола. На одном из световых форумов я прочитал похожую историю. Он написал автору сообщение, тем самым начав переписку с незнакомцем. Виртуальная собеседница рассказала, что ее зовут Настя, и она живет в том же городе. Они вместе обсуждали, что произошло, делились своими чувствами и переживаниями. В одном из сообщений Настя написала, что для того, чтобы забыть несчастную любовь, нужно найти хобби, хобби. Настя предложила Светке встретиться и вместе пойти в танцевальную студию.

1. Стоит ли договариваться о встрече с Настей? Обоснуйте свой ответ.

2. Какие могут быть негативные последствия встречи Света и ее виртуального собеседника?

3. Какие способы освещения могут защитить себя?

Правильные ответы.

1.Света не должна соглашаться на встречу, потому что не может быть уверена, кто на самом деле виртуальный собеседник.

2.Возможные негативные последствия: участвует в религиозных или экстремистских организациях, становится жертвой конкретного преступника.

3.Собираясь на свидание, Света обязательно должна сообщить любимому человеку, с кем встретиться и куда он ушел, когда вышел на связь. Назначьте встречу в людном и знакомом месте.

6. ГЛОССАРИЙ

Кибербезопасность-комплекс мер по защите программного обеспечения, информации и оборудования от злоумышленников. В частности, от несанкционированного доступа, изменения, кражи и удаления конфиденциальных данных.

Криптография-это технология шифрования информации для защиты от злоумышленников. Благодаря ему третьи стороны не могут просматривать, слушать и читать файлы без расшифровки. Данные состоят из изменяемых правил или алгоритмов, а также ключей для шифрования и дешифрования.

Электронная подпись-это технология аутентификации электронного документа, такого как договор, справка, АКТ. Это файл, который отправляется вместе с документом. Его можно передавать по открытым каналам связи. Хеш шифрует сообщение и позволяет проверить его целостность, в то время как электронная подпись защищает хеш от изменений и помогает идентифицировать личность отправителя.

Антивирус-это программа, предназначенная для обнаружения, предотвращения и удаления вирусов на вашем устройстве. Проверяет системы для повышения безопасности.

DMZ или демилитаризованная зона — это конфигурация сети, когда она находится в отдельной изолированной части, открытой для совместного использования сервера. Если это произойдет, между открытыми серверами и остальными сегментами сети не будет связи, и злоумышленники не смогут украсть данные.

Киберпространство-это контекст взаимодействия человека с потоки цифровых сигналов. Чтобы взаимодействовать с другими людьми и машинами в этой цифровой среде, люди должны выражать свои мысли в письменной форме в виде кодов и графических изображений без использования жестов, контактов и физического присутствия.

Интернет вещей-это термин, который относится к огромному и постоянно растущему набору цифровых устройств, работающих в сетях с глобальным потенциалом. Концепция Интернета вещей описывает вычислительную сеть физических объектов, оснащенную встроенными технологиями для взаимодействия друг с другом или с внешней средой.

Уязвимость-это недостаток компьютерной системы, использование которой приводит к нарушению целостности и сбою в работе системы. Уязвимости могут быть вызваны ошибками программирования, недостатками, допущенными при проектировании системы, ненадежными паролями, вредоносными программами. в результате получается.

Аппаратная закладка-это устройство в электронной схеме, которое тайно встроено в другие элементы, способные вмешиваться в работу вычислительной системы.

Прибытие на комп-результат успешной атаки на уязвимость системы. В криптографии этот термин используется для обозначения факта доступа постороннего к защищаемой информации, а также для того, чтобы вызвать у него подозрение. Чаще всего рассматривается нарушение закрытого ключа, закрытого алгоритма, цифрового сертификата, учетных записей (паролей), абонентов или других защищенных элементов, удостоверяющих личность участника обмена информацией.

Выявление уязвимостей-процесс анализа информационной системы с целью выявления возможных проблем в системе безопасности, оценки и устранения уязвимостей.

Ключ шифрования-это конфиденциальная информация (набор цифр и букв), используемая алгоритмом для шифрования и декодирования информации. Различают симметричные шифры (в данном случае один ключ, используемый для шифрования и дешифрования) и асимметричные, в которых у каждого участника есть свои ключи: открытый и закрытый.

Обнаружение атак-это процесс постоянного мониторинга информационной системы с целью обнаружения и блокировки компьютерных атак. Процесс может осуществляться через специализированное программное или аппаратное обеспечение, специалистов по кибербезопасности, облачные центры мониторинга (называемые SOC — Security Operations Center) и даже через государственные службы.

Компьютерная атака-целенаправленное несанкционированное воздействие на информацию, ресурс автоматизированной информационной системы или несанкционированный доступ к ним с использованием программных или программно-аппаратных средств. Как правило, атака использует определенную уязвимость в атакуемой информационной системе или комбинации уязвимостей

Хакер-опытный программист, который может найти быстрые и элегантные способы исправления ошибок или внесения изменений в программное обеспечение. Интересно, что в русскоязычной среде слово "хакер" часто употребляется как синоним слова "злоумышленник": человек, совершающий различные противоправные действия в области информатики.

Кибератака, киберпространственная атака (в киберпространстве) - это атака на компьютерные сети и компьютерные системы противника (специальными) программными и аппаратными средствами с целью нарушения их работы или вредоносного управления компьютерным оборудованием/инфраструктурой или нарушения целостности данных или присвоения информации (данных).

Кибербуллинг-это оскорбление, оскорбление или запугивание жертвы через социальные сети или другие электронные средства связи . киберконфликт-это конфликт в киберпространстве.

Киберпреступность-литературное название преступлений, основными средствами которых являются информационно-коммуникационные

технологии, компьютеры и компьютерные сети. Это традиционные преступления, такие как мошенничество, вымогательство (blackmail), кража личных данных, но совершаются через Интернет и/или с использованием вычислительных устройств.

Киберпреступник-пример: наша цель-шаги хакеров и киберкриминалов, взрывы на компьютерных платформах и приложениях.

Кибер-детектив-это детектив, изучающий компьютерные преступления.

Киберинцидент-вредоносная деятельность, приводящая к фактическому или возможному сбою компьютерной системы (систем) с использованием компьютерных сетей и/или к сбою (утечке, модификации) хранящихся в ней данных (информации).

Интернет-безопасность-это комплекс технических, технологических, инфраструктурных и законодательных мер, процессов и практик, обеспечивающих эффективное обнаружение и противодействие кибератакам (cyber attack), то есть защиту киберпространства (компьютерных сетей, устройств, программ и данных) от таких атак.

Рынок кибербезопасности, рынок КБ-этот рынок включает в себя такие инструменты и решения, как управление событиями нарушения безопасности (security incident management).

7. СПИСОК РЕКОМЕНДУЕМЫХ К ИСПОЛЬЗОВАНИЮ ИСТОЧНИКОВ, УЧЕБНИКОВ И ПРАВОВЫХ АКТОВ

1. Казахстан занимает 78 место из 176 стран в рейтинге по кибербезопасности.https://www.gov.kz/memleket/entities/kostanai-usunkol-audany akimat/press/news/details/612381.
2. Global Agenda Council on Cybersecurity, World Economic Forum, April 2016,//http://www3.weforum.org/docs/GAC16_Cybersecurity_WhitePaper_.pd. 22.05.2020.
3. Постановление Правительства Республики Казахстан Об утверждении государственной программы «Цифровой Казахстан». 12 декабря 2017 года. №827. //http://adilet.zan.kz/rus/docs/P1700000827. 10.03.2020.
4. Постановление Правительства Республики Казахстан Об утверждении Концепции кибербезопасности ("кибербезопасность Казахстана").: 30 июня 2017 года №407 //http://adilet.zan.kz/rus/docs/P1700000407. 10.03.2020.
5. Абучакра Р., Хури М. Эффективное правительство для нового века. Москва: Олимп-бизнес, 2020. – С. 256.
6. Global Cybersecurity Index – 2018. // https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf. 20.09.2019.
7. Исабаева С., Есениязова Б., Проблемы кибербезопасности в цифровом Казахстане. Е-Материалы 27-й ежегодной конференции NISPAcee «От разработки политики к политической практике».//www.nispa.org/files/conferences/2019/e - pdf. 13.09.2019.
8. Карпова Д., Киберпреступность: глобальная проблема и ее решение //Власть. – 2014. - №08. – С. 192
9. Зейнелгабдин А., Исабаева С., Кибербезопасность Казахстана в период цифровой трансформации //Государственный аудит. - 2019. - №4 (45). – С. 46-55.
10. Қырмызы Маршалова. Қазақстанның орнықты дамуы үшін киберқауіпсіздіктің маңызы. https://dalanews.kz/kz/article/qazaqstannin-orniqti-damui-ushin-kyberqauipsizdiktin-manizi.html.
11. Шакош Й., Шадцки Т., Построение экосистемы кибербезопасности в венгерском городе – потенциал для инновационного роста // Архитектура выбора, лежащая в основе разработки политики. – С.195-202.
12. Исабаева С.Б., Cybersecurity policy development in Kazakhstan: analysis of m-commerce user acceptance // Государственное управление и государственная служба. – 2019. - №1(68). - С 34-49.
13. Губайдуллина М. Внешнеполитическая деятельность и дипломатия в современных условиях транспарентного информационного пространства // International Relations and International Law Journal.– 2018. – Т. 79, №3. – С. 14-22.

14. Закон Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации». (С изменениями и дополнениями по состоянию на 07.01.2025 г.). https://adilet.zan.kz/kaz/docs/Z940004000

15. Закон Республики Казахстан от 06 января 2012 года № 527-V «О национальной безопасности». (С изменениями и дополнениями по состоянию на 07.01.2025 г.). https://adilet.zan.kz/kaz/docs/Z940004000

16. Исабаева С., Кармыс Г., Бексултанов А., Жусупова Г., Сравнительный анализ рейтинга стран по цифровизации и кибербезопасности: проблемы и возможности // Казахстан – Спектр. – 2018. - №3(85). – С. 23-36.

17. Соколов М.С. Кибернетическая безопасность – понятие, значение и эволюция // http://lib.znate.ru/download/docs59946/59946.doc.

18. Drage-Arianson K., Crouch D., Cybersecurity: Building Resilience from the Inside Out // Chemical Engineering. – 2018. – Vol. 125(10). - P. 65–68.

19. Татаринова Л., Соотношение понятий «информационная безопасность»,«защита информации» и «кибербезопасность»,«киберзащита» по законодательству Республики Казахстан // Вестник КазНУ. Серия юридическая. – 2019. – Т. 67. – №. 3. – С. 60-64.

20. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 1) // Вопросы кибербезопасности. 2013. № 1(1). С.2-9.

21. Жумагалиев А. Обзор The Boston Consulting Group. // Специальный выпуск: Казахстан, обзор. 2018. С.1-66.

22. Паршин С.А., Горбачев Ю.Е., Кожанов Ю.А. Кибервойны - реальная угроза национальной безопасности. М.: Изд-во КРА-САНД, 2011. 96 с.

23. Валиахметова Г. Н. Обеспечение национальной кибербезопасности в условиях виртуальных войн XXI в.: опыт Исламской Республики Иран / Г. Н. Валиахметова // Известия Уральского федерального университета. Сер. 3, Общественные науки. — 2016. — № 2 (152). — С. 87-97.

24. Жумагалиев А. The Boston Consulting Group review. // Специальный выпуск: Казахстан, обозрение. 2018. С.1-66.

25. Исабаева С.Б. Стратегии кибербезопасности разных стран в эпоху глобальной цифровизации // Тенденции мировых интеграционных процессов: вызовы и возможности: сб. матер. междунар. науч. конф.. – Нур-Султан, 2019. – С. 182-194.

26. Постановление Правительства Республики Казахстан от 28 марта 2023 года № 269 "Об утверждении Концепции развития цифровой трансформации, информационно - коммуникационных технологий и кибербезопасности на 2023-2029 годы".

27. Закон Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информационной безопасности, информатизации и цифровых активов» от 11 декабря 2023 года № 44-VIII.

28. Закон Республики Казахстан от 21 мая 2013 года № 94-V "О персональных данных и их защите".

29. Конвенция о компьютерных преступлениях (Конвенция Совета Европы о киберпреступности, Convention on Cybercrime CETS № 185) (Будапешт, 23 ноября 2001 года).

30. Закон Республики Казахстан от 5 июля 2004 года №567-II «О связи» (с изменениями и дополнениями от 22.02.2025).

31. Земскова И. А. Трансформация качества государственных услуг под влиянием цифровизации государственных органов //Вестник Саратовского государственного социально-экономического университета. – 2018. – №. 3 (72).– С. 23–28.

32. Послание Президента РК К. Токаева народу Казахстана от 1 сентября 2021 года «Единство народа и системные реформы – прочная основа процветания страны».

33. Послание Президента РК К. Токаева народу Казахстана от 1 сентября 2021 года «Единство народа и системные реформы – прочная основа процветания страны».

34. Ескендір З., Киберпол – жаңа тергеу амалы. https://egemen.kz/article/345462-kiberpol-%E2%80%93-dganha-tergeu-amaly.

35. Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V (с изменениями и дополнениями по состоянию на 09.09.2024г.). https://adilet.zan.kz/kaz/docs/U090000858_

36. Конституция Республики Казахстан (принята на республиканском референдуме 30 августа 1995 года) (с изменениями и дополнениями по состоянию на 19.09.2022 г.). [Электронный ресурс]-URL: //https://adilet.zan.kz/kaz/docs/K950001000.

37. Кубышкин Алексей Викторович. Международно-правовые проблемы обеспечения информационной безопасности государства : Дис. ... канд. юрид. наук : 12.00.10 : Москва, 2002.-193 с.

38. Осипенко А. Л. Государственно-частное партнерство в сфере противодействия киберпреступности //Вестник Воронежского института МВД России. – 2016. – №. 4.

39. Указ Президента Республики Казахстан от 14 ноября 2011 года № 174 "О Концепции информационной безопасности Республики Казахстан до 2016 года".

40. Закон Республики Казахстан от 29 мая 2007 года N 257 "О ратификации Соглашения между правительствами государств-членов Шанхайской организации сотрудничества о взаимодействии при оказании помощи в ликвидации чрезвычайных ситуаций".

41. Бексултанов А., Кармыс Г., Исабаева С., Цифровизация экономики – фактор повышения конкурентоспособности Республики Казахстан. // Сб. 14 междунар. науч.-практ. конф. студентов, аспирантов, магистрантов «Цифровые технологии в экономике и управлении: научный взгляд молодых. 2018. С. 596- 599.

42. Клименко П., Клименко И., Цифровая экономика современного Казахстана: новые вызовы //Черноморская конференция-2019. – 2019. – С. 98- 99.

43. Мусабаев Р., Касымжанов Б., Калиева Г., Ибраева В., Разработка Информационных технологий и систем для стимулирования устойчивого развития личности как одна из основ развития Цифрового Казахстана // Проблемы оптимизации сложных систем. – 2018. – С. 39-46.

44. Головенчик Г. Г. Рейтинговый анализ уровня цифровой трансформации экономик стран ЕАЭС и ЕС //Цифровая трансформация. – 2018. – №. 2. – С. 5-18.

45. Об утверждении Стратегии кибербезопасности финансового сектора Республики Казахстан на 2020-2022 годы «Совместное постановление Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 20 июля 2020 года № 69 и Правления Национального Банка Республики Казахстан» от 20 июля 2020 года № 89.

46. Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832.

47. Кармыс Г., Бексултанов А., Исабаева С., Джусупова Г.. Сравнительный анализ государственного подхода к цифровизации Казахстана и России //Вестник университета Туран. – 2018. – №. 3. – С. 197-201.

48. Закон Республики Казахстан от 8 февраля 2003 года N 387 "О чрезвычайном положении".

49. Казахстанский путь-2050: единая цель, единые интересы, единое будущее послание Первого Президента Республики Казахстан Н. А. Назарбаева народу Казахстана, г. Астана, 17 января 2014 года.

50. Указ Президента Республики Казахстан от 10 сентября 2019 года № 152 "О мерах по реализации Послания Президента РК К. Токаева народу Казахстана от 2 сентября 2019 года «Конструктивный общественный диалог – основа стабильности и процветания Казахстана».

51. Притворова Т., Жашкенова Р., Системообразующие характеристики цифровой экономики // Найновите Постижения на Европейската Наука -2019. – 2019. – С. 50.

52. Баймухамедов М., Баймухамедова Г., Аймурзинов М., Технологическая модернизация экономики страны на основе реализации госпрограммы «Цифровой Казахстан» // Аграрный вестник Урала. – 2019. – №. 2 (181). – С. 42-45.

53. Указ Президента Республики Казахстан от 10 сентября 2019 года № 152 "О мерах по реализации Послания Президента РК К. Токаева народу Казахстана от 2 сентября 2019 года «Конструктивный общественный диалог – основа стабильности и процветания Казахстана".

54. Краузе Н., Алимбетов У., Битенова Б., Самусенко Е., Цифровизация: формирование и развитие в Республике Казахстан. // Вестник университета Туран. – 2019. - № 4. – С. 211-217.

55. Жетисов А. Ж. О необходимости защиты информации в сфере деятельности, связанной с выявлением и раскрытием преступлений // Актуальные проблемы современности. 2018. № 3 (21). С. 68-72.

56. Ханов Т. А., Нуркеев А. Ж. Современные подходы к определению компьютерной преступности и особенности компьютерных преступлений //Известия Алтайского государственного университета. 2017. № 6 (98). С. 105-111.

57. Шульгин Е.П., Сапарғалиев Ж.Н., Досымбетов Е.О., Тафинцев П.А. Компьютерлік ақпарат саласындағы алаяқтықты тергеудің ерекшеліктері: оқу құралы. – Қарағанды: Қазақстан Республикасы ІІМ Бәрімбек Бейсенов атындағы Қарағанды академиясы, 2023. – 53 б.

58. Абдуллаев А.А., Аубакирова А.М., Касымов А.К. Административные аспекты кибербезопасности в Республике Казахстан: состояние и перспективы развития // Вестник Академии правоохранительных органов. — 2022. — № 3 (90). — С. 18-28.

59. Исабаева С. Тенденции инновационной деятельности Казахстана и стран СНГ: сравнительный анализ // Матер. 5-й междунар. науч.-практ. конф. «Национальная правовая система Республики Таджикистан и стран СНГ: анализ тенденций и перспектив развития». – Душанбе, 2017. – С. 187 - 192.

60. Кодекс Республики Казахстан Об административных правонарушениях от 5 июля 2014 года № 235-V ЗРК. (С изменениями и дополнениями по состоянию на 13.12.2024 г.). https://adilet.zan.kz/kaz/docs/U090000858_

61. Маулетбай С., Как «вирус от Генпрокуратуры» помог разбогатеть хакерам, 2016.// https://informburo.kz/stati/kak-virus-ot-genprokuratury-pomog-razbogatet-hakeram.html. 23.07.2019.

62. Сейткулов Е., Информационная безопасность Республики Казахстан: состояние и перспективы. 2016. // http://www.enu.kz/ru/info/novosti-enu/novosti- nauki/45582/. 09.09.2019.

З.З. НҰРЫШ
«ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ»
Учебно-методическое пособие

Сдано в печать «____»____2025 года.
Формат 60х84 1|16
Объем _____ п.л.
Тираж ____ шт.
Заказ №_____
ТОО «ADAL KITAP»