КОСТАНАЙСКАЯ АКАДЕМИЯ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ КАЗАХСТАН
ИМЕНИ ШРАКБЕКА КАБЫЛБАЕВА

Бримжанова С.С.

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ДЕЯТЕЛЬНОСТИ ОВД

Учебное пособие

Костанай, 2024

УДК 004 (075.8)
ББК 32.973 я73
Б 87

Рекомендовано Ученым советом Костанайской академии
МВД Республики Казахстан им. Ш. Кабылбаева

Рецензенты:
доцент кафедры педагогики и психологии Костанайской академии МВД Республики Казахстан им. Ш. Кабылбаева, кандидат педагогических наук **Жандарбекова Г.Б.,**
доктор физико-математических наук, проректор по академическим вопросам Кокшетауского университета им. Ш. Уалиханова **Медетов Н.А.**

Бримжанова С.С.
Б 87 Современные информационные технологии в деятельности ОВД: учебное пособие / авт.-сост. Бримжанова С.С. - Костанай: Костанайская академия МВД Республики Казахстан им. Ш. Кабылбаева, 2024. – 103 с.

ISBN 978-601-367-005-8

Учебное пособие представляет собой комплексный материал, который освещает вопросы, связанные с применением информационных технологий в деятельности правоохранительных органов. Рассматриваются вопросы о применении электронных систем для обработки документов и ведения учета; кибербезопасность и информационная безопасность.

Логика построения учебного пособия обеспечивается последовательностью, системностью и взаимообусловленностью изложения ключевых аспектов информационных технологий в деятельности ОВД и ориентирована на широкий охват необходимого объема знаний, служащих основой для дальнейшей профессиональной подготовки обучающихся.

Учебное пособие предназначено для курсантов, студентов, магистрантов, докторантов, а также преподавателей высших учебных заведений.

УДК 004 (075.8)
ББК 32.973 я73

ISBN 978-601-367-005-8

СОДЕРЖАНИЕ

СОКРАЩЕНИЯ И ОБОЗНАЧЕНИЯ

МВД	Министерство внутренних дел
РК	Республика Казахстан
ОВД	Органы внутренних дел
ВПО	Вредоносное программное обеспечение
ИБД	Интегрированный банк данных
ИИ	Искуственный интеллект
СИО ПСО	Система информационного обмена правоохранительных, специальных государственных и иных органов
ЕРДР	Единый реестр досудебных расследований
ЕРАП	Единый реестр административных производств
АП	Административная практика
ИБ	Информационная безопасность
ИТ	Информационные технологии
СКОВ	Соблюдение нормативных требований
LAN	Локальные сети
WAN	Глобальные сети
VPN	Виртуальные частные сети

ВВЕДЕНИЕ

В современном информационном обществе информационные технологии стали неотъемлемой частью работы органов внутренних дел по всему миру. В эпоху цифровой трансформации и быстрого развития технологий, применение современных информационных решений стало ключевым фактором в обеспечении эффективности и оперативности деятельности правоохранительных органов. Информационные технологии становятся мощным инструментом в борьбе с преступностью, обеспечении безопасности граждан и создании эффективной системы правопорядка.

Цель данного учебного пособия – предоставить специалистам и всем заинтересованным лицам полное представление об информационных технологиях, их роли и значимости в деятельности органов внутренних дел. Органы внутренних дел сталкиваются с постоянно меняющимися вызовами и сложностями, связанными с обеспечением безопасности общества. Благодаря информационным технологиям, они получают возможность собирать, обрабатывать и анализировать большие объемы информации, что помогает в принятии взвешенных и оперативных решений. Современные системы электронного учета и контроля, базы данных и информационные системы позволяют эффективно управлять информацией о преступлениях, преступниках и жертвах, а также обеспечивать быстрый доступ к необходимым данным.

Однако, развитие информационных технологий также сопряжено с вызовами в области кибербезопасности. С увеличением количества цифровых угроз и киберпреступлений, органы внутренних дел должны активно применять современные методы защиты и обеспечения информационной безопасности, чтобы предотвратить и расследовать преступления в сети.

При подготовке учебного пособия автор ориентировался на действующие законодательные и подзаконные нормативные правовые акты, включая ведомственные нормативные акты МВД Республики Казахстан, на зарубежные научные источники по общим проблемам развития информационных технологий, а также труды известных ученых и практиков, внесших существенный вклад в теорию и практику управления правоохранительных органов.

Учебное пособие направлено на подготовку будущих специалистов, способных эффективно работать в современных и изменяющихся условиях профессиональной практики. В настоящее время информационные технологии играют ведущую роль в деятельности органов внутренних дел, поэтому их освоение и применение являются неотъемлемой частью профессиональной подготовки.

Важной задачей данного пособия является формирование у обучающихся профессионального мировоззрения, понимания смысла и роли информационных технологий в деятельности органов внутренних дел. Мы стремимся установить связь между сущностью и содержанием работы правоохранительных органов, их формами и направлениями деятельности, а

также влиянием информационных технологий на эффективность выполнения служебных обязанностей.

В заключение, данное учебное пособие имеет целью удовлетворение потребностей общества в высококвалифицированных специалистах, способных применять разнообразные информационно–коммуникационные технологии.

ТЕМА 1. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ОВД

Цель: изучить основные термины информационных технологий в деятельности органов внутренних дел, рассмотреть их роль в современном контексте и исследовать перспективы их развития.

План:

1. Определение информационных технологий и их значение для эффективного функционирования органов внутренних дел.
2. Роль информационных технологий в усилении оперативно-розыскной деятельности, обеспечении безопасности и содействии в расследованиях преступлений.
3. Роль информационных технологий в обеспечении безопасности.
4. Роль информационных технологий в расследованиях преступлений.

1. Определение информационных технологий и их значение для эффективного функционирования органов внутренних дел.

В современном обществе информационные технологии стали неотъемлемой частью жизни и профессиональной деятельности, и правоохранительные органы не являются исключением.

Информация - это факты, данные, понимание или знания, которые получаются или передаются через коммуникационные средства или другие формы передачи. Она представляет собой сведения, которые могут быть использованы для принятия решений, понимания ситуации или получения знаний об определенном предмете или явлении.

Информация может быть представлена в различных формах, таких как текст, числа, графики, изображения или звук. Она может быть структурированной или неструктурированной, а также может иметь различные уровни значимости и конфиденциальности.

Информация играет важную роль во многих областях жизни, включая науку, бизнес, образование, массовые коммуникации и технологии. Она служит основой для принятия решений, планирования, коммуникации, исследований и инноваций.

Защита информации, ее конфиденциальность, целостность и доступность являются важными аспектами информационной безопасности. Корректная и достоверная информация является ценным ресурсом, и ее защита становится все более важной в современном информационном обществе.

Информационные технологии – это совокупность методов, инструментов и процессов, связанных со сбором, обработкой, хранением, передачей и использованием информации [1].

Они включают в себя широкий спектр технических и программных

средств, а также систем и протоколов, которые обеспечивают обработку информации с высокой скоростью и точностью.

Для органов внутренних дел Республики Казахстан информационные технологии имеют огромное значение. Они играют ключевую роль в современной оперативно-розыскной деятельности, обеспечивая сбор, анализ и обработку информации, необходимой для предотвращения и раскрытия преступлений. Благодаря информационным технологиям, правоохранительные органы могут эффективно управлять оперативной информацией, обеспечивать безопасность граждан и бороться с преступностью.

Одним из примеров использования информационных технологий в деятельности органов внутренних дел является использование компьютерных систем и баз данных для хранения информации о преступлениях и преступниках. Это позволяет быстро и эффективно осуществлять поиск и анализ данных, а также сопоставлять информацию с другими базами данных для выявления связей между различными преступными событиями.

Еще одним важным аспектом информационных технологий в деятельности органов внутренних дел является использование систем видеонаблюдения и распознавания лиц. Эти технологии позволяют осуществлять контроль за общественным порядком, предотвращать преступления и идентифицировать подозреваемых. Благодаря развитию информационных технологий, возможности видеонаблюдения значительно расширились, а системы распознавания лиц стали более точными и эффективными.

Однако, информационные технологии не только облегчают работу органов внутренних дел, но и представляют определенные вызовы и угрозы. С развитием технологий, преступники также находят новые способы использования информационных технологий для совершения преступлений. Киберпреступления, хакерские атаки и распространение незаконного контента в сети Интернет стали серьезными вызовами для правоохранительных органов. Поэтому важно, чтобы органы внутренних дел постоянно развивали свои информационные технологии и обеспечивали кибербезопасность для защиты информации и предотвращения преступлений в сфере информационных технологий.

В заключение, информационные технологии играют важную роль в эффективном функционировании органов внутренних дел Республики Казахстан. Они позволяют обеспечивать оперативность и точность в обработке информации, совершенствовать методы борьбы с преступностью и повышать безопасность граждан. Однако, необходимо учитывать и угрозы, связанные с использованием информационных технологий, и принимать меры по защите информации и борьбе с киберпреступностью. Развитие информационных технологий и их эффективное использование являются неотъемлемой частью работы органов внутренних дел и способствуют достижению целей обеспечения общественной безопасности и правопорядка в Республике Казахстан.

2. Роль информационных технологий в усилении оперативно-розыскной деятельности, обеспечении безопасности и содействии в расследованиях преступлений.

Системы видеонаблюдения и распознавания лиц для контроля общественного порядка и идентификации подозреваемых.

1. Роль систем видеонаблюдения [2]:

Системы видеонаблюдения используются для контроля общественного порядка на улицах, в общественных местах, в транспорте и других общественных пространствах. Они помогают предотвращать преступления, обнаруживать нарушения и быстро реагировать на происшествия.

Системы видеонаблюдения обеспечивают постоянную запись происходящего, что позволяет восстанавливать события, проводить расследования и использовать записи в качестве доказательств в судебных процессах.

2. Роль систем распознавания лиц:

Системы распознавания лиц позволяют автоматически идентифицировать лица на основе сравнения с базой данных фотографий или видеозаписей. Они способствуют более быстрой и точной идентификации подозреваемых, пропавших людей или лиц, находящихся в розыске.

Системы распознавания лиц могут быть интегрированы с системами видеонаблюдения, что позволяет автоматически сопоставлять лица, заснятые камерами, с базой данных и выдавать предупреждения о потенциальных угрозах или совпадениях с подозреваемыми.

Например:

1. В Казахстане системы видеонаблюдения активно используются для контроля общественного порядка и обеспечения безопасности городских территорий. В городе Астана установлены множество камер наблюдения, которые позволяют мониторить общественные пространства и быстро реагировать на возможные происшествия.
2. В систему видеонаблюдения метрополитена Алматы интегрированы системы распознавания лиц. Это позволяет эффективно контролировать пассажиров и идентифицировать подозреваемых лиц в случае возникновения преступных ситуаций.
3. Примером успешного использования системы распознавания лиц в Казахстане является система «Qoldau.ai», разработанная в Алматы. Она использует искусственный интеллект для автоматического распознавания лиц на видеозаписях и помогает органам правопорядка быстро идентифицировать подозреваемых и расследовать преступления.

Системы видеонаблюдения и распознавания лиц играют значительную роль в обеспечении контроля общественного порядка и идентификации подозреваемых. Они обеспечивают непрерывный мониторинг общественной среды, предупреждают преступления и способствуют расследованию. Примеры применения этих систем в Республике Казахстан демонстрируют их эффективность и важность для обеспечения общественной безопасности.

Использование специализированного программного обеспечения для анализа больших объемов данных и выявления связей между преступниками и их деятельностью.

В современной эпохе информационных технологий органы правопорядка сталкиваются с огромными объемами данных, которые требуют систематического анализа и обработки для эффективного борьбы с преступностью. Использование специализированного программного обеспечения позволяет автоматизировать процесс анализа данных и выявлять скрытые связи и закономерности, что способствует более эффективному расследованию преступлений.

1. Значение анализа больших объемов данных:

Современные органы правопорядка сталкиваются с огромными объемами данных, включающими информацию о преступлениях, подозреваемых, свидетелях, местах происшествий и других связанных факторах.

Анализ больших объемов данных позволяет выявлять скрытые связи и закономерности, которые могут указывать на схемы преступной деятельности, организованные группы или преступные сети.

Специализированное программное обеспечение для анализа данных помогает сократить время и усилия, затрачиваемые на обработку информации, и повышает эффективность расследования.

2. Примеры специализированного программного обеспечения:

IBM i2 Analyst's Notebook [3]: Это программное обеспечение предназначено для анализа сложных данных и выявления связей между преступниками и их деятельностью. Оно позволяет создавать графические модели, визуализирующие связи между лицами, событиями и объектами, а также проводить анализ текстовых и числовых данных.

Palantir Gotham: Эта платформа анализа данных предоставляет возможность объединять, структурировать и анализировать различные типы данных, включая тексты, изображения, географические данные и другие. Она позволяет исследователям обнаруживать скрытые связи и паттерны, которые могут быть важными для расследования преступлений.

SAS Visual Investigator: Это программное обеспечение предназначено для анализа данных и расследования преступлений. Оно объединяет данные из различных источников и предоставляет функциональные возможности для анализа, визуализации и представления результатов.

Использование специализированного программного обеспечения для анализа больших объемов данных является важным инструментом для органов правопорядка. Оно позволяет эффективно обрабатывать и анализировать данные, выявлять связи между преступниками и их деятельностью, а также обнаруживать скрытые паттерны и закономерности. Примеры программного обеспечения, такие как IBM i2 Analyst's Notebook, Palantir Gotham и SAS Visual Investigator, демонстрируют возможности современных технологий в области анализа данных для успешного борьбы с преступностью и обеспечения безопасности общества.

Электронное хранение и обработка оперативной информации для быстрого доступа и обмена данными между различными структурами правоохранительных органов.

В правоохранительных органах информация играет ключевую роль и является одним из основных ресурсов для выполнения их функций. Информация в правоохранительных органах представляет собой сведения и данные, полученные из различных источников, которые имеют отношение к преступлениям, правонарушениям, подозреваемым, потерпевшим, свидетелям и другим аспектам, связанным с обеспечением общественной безопасности и выполнением законодательства.

Информация в правоохранительных органах может включать [4]:

1. Оперативную информацию: Это конфиденциальные сведения и данные, полученные из разведывательной деятельности, об аффилированных лицах, преступных сетях, планах преступлений и других событиях, которые требуют немедленного реагирования со стороны правоохранительных органов. Оперативная информация является важным инструментом оперативно-розыскной деятельности и позволяет предотвращать преступления и разоблачать преступников.

2. Служебную информацию: Это информация, которая используется для внутреннего управления и оперативного планирования деятельности правоохранительных органов. Она может включать данные о структуре организации, кадровом составе, распределении ресурсов, бюджете, организационных процессах и других аспектах, связанных с эффективным функционированием правоохранительной системы.

3. Информацию о преступлениях и правонарушениях: Включает данные о совершенных преступлениях, их характеристиках, обстоятельствах, методах и мотивах, а также о потерпевших, свидетелях и подозреваемых. Эта информация является основой для расследования преступлений и принятия соответствующих мер по привлечению виновных к ответственности.

Информация в правоохранительных органах должна быть достоверной, актуальной, конфиденциальной и обрабатываться в соответствии с законодательством о защите данных и приватности. Она служит основой для принятия оперативных решений, планирования действий, анализа преступных ситуаций и сотрудничества между различными структурами правоохранительных органов.

В современном информационном обществе оперативная информация играет важную роль в борьбе с преступностью и обеспечении безопасности общества. Электронное хранение и обработка оперативной информации позволяют эффективно управлять данными, обеспечивать их доступность и обмен между различными структурами правоохранительных органов.

1. Значение электронного хранения и обработки оперативной информации:

Оперативная информация является ключевым ресурсом для правоохранительных органов. Она включает данные о преступлениях, подозреваемых, жертвах, свидетелях, связях между лицами и другие важные

сведения.

Электронное хранение и обработка оперативной информации позволяют сохранять данные в электронном виде, обеспечивать их быстрый доступ и обмен между различными структурами правоохранительных органов.

Эффективное использование электронного хранения и обработки оперативной информации способствует более оперативному реагированию на преступные события, сокращению времени расследования и улучшению сотрудничества между различными организациями.

2. Примеры систем электронного хранения и обработки оперативной информации:

Система, Автоматизированная система коммерческой информации и заявок: используется правоохранительными органами для хранения и обработки оперативной информации. Позволяет эффективно управлять данными, обеспечивать доступ и обмен между различными структурами органов внутренних дел.

Система, Единой базы данных: Интегрированная система хранения и обработки оперативной информации, которая объединяет данные из различных источников и обеспечивает их доступность для сотрудников правоохранительных органов.

Система Единая информационно-аналитическая система правоохранительных органов: Разработана для оперативного хранения, анализа и обмена информацией между различными структурами правоохранительных органов Казахстана. Обеспечивает эффективное взаимодействие между органами и повышает оперативность расследования преступлений.

В современном мире электронное хранение и обработка оперативной информации играют важную роль в деятельности правоохранительных органов. Они позволяют обеспечить быстрый доступ и обмен данными между различными структурами, улучшить оперативно-розыскную деятельность, обеспечить безопасность общества и эффективность расследования преступлений. Примеры систем демонстрируют значимость и практическую реализацию электронного хранения и обработки оперативной информации в Казахстане. Эти системы способствуют сотрудничеству между структурами правоохранительных органов и обеспечивают эффективное использование оперативной информации для обеспечения общественной безопасности.

Коммуникационные системы, включая радиосвязь и системы передачи данных, для оперативной связи между сотрудниками правоохранительных органов.

Коммуникационные системы являются неотъемлемой частью работы правоохранительных органов и играют важную роль в оперативной связи между их сотрудниками. Они обеспечивают быстрое и надежное обмен информацией, координацию действий и оперативное реагирование на происшествия.

Коммуникационные системы включают в себя различные технологии и устройства, предназначенные для передачи информации и обеспечения связи между сотрудниками правоохранительных органов. Они могут включать

радиосвязь, системы передачи данных, телефонию, интернет-связь и другие средства связи [5].

Основные принципы и требования к коммуникационным системам:

1. *Быстрота и надежность:* Коммуникационные системы должны обеспечивать мгновенный обмен информацией и быть надежными в условиях оперативной деятельности правоохранительных органов.

2. *Конфиденциальность и безопасность:* Коммуникационные системы должны обеспечивать защиту передаваемой информации и предотвращать несанкционированный доступ к ней.

3. *Покрытие и доступность:* Системы связи должны иметь широкий охват и быть доступными в различных районах и условиях, включая отдаленные и труднодоступные места.

Примеры коммуникационных систем в правоохранительных органах:

1. *Радиосвязь:* Использование радиосвязи позволяет оперативно передавать голосовую информацию между сотрудниками на местах происшествий, патрулирующими автомобилями и другими оперативными группами.

2. *Системы передачи данных:* С помощью систем передачи данных сотрудники правоохранительных органов могут обмениваться текстовой информацией, документами, фотографиями и видеоматериалами для оперативного анализа и принятия решений.

3. *Мобильные телефоны:* Использование мобильных телефонов позволяет сотрудникам быть доступными для связи в любое время и в любом месте, обеспечивая оперативную коммуникацию.

Коммуникационные системы играют ключевую роль в оперативной связи между сотрудниками правоохранительных органов. Они обеспечивают быстрый обмен информацией, координацию действий и эффективное реагирование на происшествия. Правильное использование и развитие коммуникационных систем способствует повышению эффективности работы правоохранительных органов и обеспечению безопасности общества.

3. Роль информационных технологий в обеспечении безопасности.

Информационные технологии (ИТ) играют ключевую роль в обеспечении безопасности в современном мире. С развитием технологий и расширением информационного пространства возникают новые вызовы и угрозы, которые могут быть эффективно преодолены с помощью информационных технологий.

Основные понятия:

Защита в правоохранительных органах Республики Казахстан относится к комплексу мер и действий, направленных на обеспечение безопасности и надежности их деятельности, информационных систем, персонала и общественного порядка. Защита в правоохранительных органах имеет целью предотвращение и пресечение противоправных действий, обеспечение сохранности информации и эффективность работы органов в целом [6].

Несанкционированный доступ в правоохранительных органах Республики Казахстан означает получение или попытку получения доступа к информации, ресурсам или системам органов без соответствующих разрешений или полномочий [7]. Это может быть совершено как внутри органов самими сотрудниками, так и внешними лицами.

Несанкционированный доступ является нарушением информационной безопасности и может иметь серьезные последствия для деятельности правоохранительных органов. В результате такого доступа злоумышленники могут получить конфиденциальную оперативную информацию, нарушить целостность данных, повлиять на работу системы или использовать полученную информацию для незаконных целей.

Информационные системы в органах внутренних дел Республики Казахстан представляют собой комплекс программных и аппаратных средств, используемых для сбора, обработки, хранения и передачи информации в рамках деятельности правоохранительных органов. Они служат основой для эффективного функционирования и организации работы органов внутренних дел Республики Казахстан.

Шифрование представляет собой процесс преобразования исходного текста или данных в зашифрованный формат с использованием определенного алгоритма и ключа. Это позволяет обеспечить защиту информации от несанкционированного доступа и чтения [8].

Аутентификация является процессом проверки и подтверждения подлинности личности или учетных данных пользователя для доступа к информационным системам и ресурсам. Она выполняется для обеспечения безопасности и контроля доступа к конфиденциальной информации, а также для предотвращения несанкционированного использования и злоупотребления привилегиями [9].

Идентификация – это процесс проверки подлинности личности, устройства, приложения или другого субъекта в информационной системе. Она позволяет установить, что субъект является тем, за кого он себя выдает, и предоставить соответствующие привилегии или доступ к ресурсам [10].

Вирусы представляют собой вредоносные программы или коды, созданные для нанесения вреда информационным системам и компьютерам, используемым в работе правоохранительных органов. Вирусы могут быть разработаны с целью проникновения, разрушения, изменения или кражи данных, а также нарушения работы компьютерной сети [11].

Хакерские атаки представляют собой несанкционированные попытки проникновения в информационные системы и сети правоохранительных органов Республики Казахстан со стороны злоумышленников. Целью таких атак может быть получение конфиденциальной информации, нанесение ущерба системе, изменение данных, нарушение работы или использование системы в противозаконных целях [12].

Угрозы относятся к потенциальным событиям, действиям или ситуациям, которые могут нанести вред безопасности, оперативной деятельности и нормальному функционированию органов внутренних дел.

Угрозы могут исходить из различных источников и иметь различные характеристики [13].

Киберугрозы относятся к потенциальным атакам и инцидентам в киберпространстве, которые могут нанести вред информационным системам, сетям и ресурсам органов внутренних дел Республики Казахстан. Киберугрозы имеют различные формы и могут происходить из разных источников, включая злоумышленников, хакеров, киберпреступников, государственные и нетрадиционные акторы [14].

Утечка данных представляет собой несанкционированное раскрытие или потерю конфиденциальной информации, которая относится к оперативной деятельности, расследованиям, персональным данным граждан или другим чувствительным данным, связанным с правоохранительными органами. Утечка данных может происходить как намеренно, с целью нанесения вреда или выгоды третьей стороне, так и случайно, в результате ошибок или неправильной обработки информации.

Киберпространство представляет собой виртуальную среду, состоящую из информационных систем, сетей, компьютеров и других электронных устройств, которая используется для обмена информацией и взаимодействия субъектов правоохранительной деятельности. Киберпространство обладает своими особенностями и правилами функционирования [15].

Кибератаки представляют собой злонамеренные действия в киберпространстве, направленные на нарушение функционирования информационных систем, сетей и компьютеров правоохранительных органов, а также на получение несанкционированного доступа к конфиденциальной информации или нанесение ущерба оперативной деятельности.

Киберпреступники — это лица или группы, которые совершают преступления с использованием компьютерных и информационных технологий. Они используют свои навыки и знания в области информационной безопасности для осуществления незаконных действий в киберпространстве [16].

Кибербуллинг представляет собой форму киберпреступности, которая характеризуется использованием информационно-коммуникационных технологий для запугивания, угроз, оскорблений, шантажа и других форм психологического насилия над людьми. Он осуществляется через различные онлайн-платформы, такие как социальные сети, форумы, мессенджеры и электронная почта [17].

Безопасность означает обеспечение и поддержание общественного порядка, защиту граждан, предотвращение преступлений и реагирование на них. Она представляет собой состояние, при котором люди, общество и его институты находятся в защищенном состоянии от угроз, рисков и незаконных действий.

Безопасность может иметь несколько аспектов [18]:

1. Общественная безопасность: Включает в себя защиту жизни, здоровья и имущества граждан. Правоохранительные органы обеспечивают общественный порядок, предотвращают и расследуют преступления, и

реагируют на чрезвычайные ситуации, такие как природные катастрофы или террористические акты.

2. *Национальная безопасность:* Связана с защитой государства от внешних и внутренних угроз. Правоохранительные органы осуществляют контроль границ, борются с терроризмом, подрывной деятельностью и другими формами угроз национальной безопасности.

3. *Кибербезопасность:* Связана с защитой информационных систем и данных от киберугроз. Правоохранительные органы борются с киберпреступностью, предотвращают хакерские атаки, защищают конфиденциальность и целостность информации.

4. *Личная безопасность сотрудников правоохранительных органов:* Правоохранительные органы заботятся о безопасности своих сотрудников, предоставляя им необходимую защиту и средства самообороны.

Безопасность в правоохранительных органах является комплексным и многогранным понятием, требующим координации и сотрудничества различных служб и специалистов. Она направлена на создание безопасной и стабильной среды для развития общества и защиты прав и интересов граждан.

Роль информационных технологий в обеспечении безопасности:

1. *Сбор, анализ и обработка данных:* Информационные технологии позволяют собирать, анализировать и обрабатывать большие объемы данных, что помогает выявлять угрозы, анализировать тренды и прогнозировать возможные инциденты. Примеры включают системы мониторинга и анализа данных, которые позволяют обнаружить аномальное поведение или потенциальные угрозы.

2. *Системы видеонаблюдения [19]:* Видеонаблюдение является важным компонентом систем обеспечения безопасности. Современные системы видеонаблюдения, основанные на ИТ, позволяют контролировать общественные места, объекты критической инфраструктуры, а также обнаруживать и распознавать лица подозреваемых. Они способствуют превентивным мерам безопасности и улучшают возможности оперативного реагирования.

3. *Кибербезопасность [20]:* С увеличением числа киберугроз и киберпреступлений важным аспектом обеспечения безопасности становится защита информационных систем и данных от несанкционированного доступа, вирусов и хакерских атак. ИТ-инфраструктура должна быть защищена с помощью современных методов аутентификации, шифрования, межсетевых экранов и систем обнаружения вторжений.

4. *Системы управления кризисными ситуациями [21]:* IT-системы позволяют правоохранительным органам эффективно управлять кризисными ситуациями, такими как природные бедствия, террористические акты или массовые беспорядки. Они обеспечивают координацию действий, обмен информацией и оперативную связь между различными службами и структурами.

Примеры применения информационных технологий в обеспечении безопасности:

– Система электронного контроля доступа, позволяющая регулировать доступ к ограниченным зонам и объектам.

– Системы распознавания лиц, позволяющие идентифицировать подозреваемых на основе сравнения их лиц с базой данных.

– Системы автоматического распознавания номерных знаков автомобилей для обнаружения, угнанных или подозрительных транспортных средств.

– Системы мониторинга социальных медиа, чтобы выявлять потенциальные угрозы или признаки преступной деятельности.

Информационные технологии играют важную роль в обеспечении безопасности, предоставляя средства для сбора, анализа и обработки данных, контроля общественного порядка, защиты информационных систем и координации действий в кризисных ситуациях. Правильное использование и развитие информационных технологий помогает повысить эффективность работы правоохранительных органов и обеспечить безопасность общества.

Кибербезопасность в правоохранительных органах относится к области защиты информационных систем, данных и сетей от киберугроз и киберпреступности. Она включает в себя меры и практики, направленные на предотвращение, выявление и реагирование на кибератаки, а также обеспечение конфиденциальности, целостности и доступности информации [22].

Основные составляющие информационной безопасности

Конфиденциальность информации:

Конфиденциальность информации относится к обеспечению ее защиты от несанкционированного доступа и раскрытия. Она гарантирует, что информация доступна только тем лицам, которые имеют право на ее получение, и что она не попадает в руки или не используется несанкционированными лицами или организациями. Защита конфиденциальности может осуществляться путем применения шифрования, контроля доступа и других мер безопасности.

Примеры конфиденциальной информации в правоохранительных органах включают следующее [23]:

1. Персональные данные граждан, такие как их имена, адреса, данные паспортов и другая личная информация.

2. Оперативная информация, связанная с расследованиями преступлений, которая может содержать данные о подозреваемых, свидетелях, информантах и других конфиденциальных сведениях.

3. Служебные документы, содержащие сведения о тактике, стратегии и оперативной деятельности правоохранительных органов.

Целостность информации [24]:

Целостность информации относится к ее целостности и неприкосновенности. Она гарантирует, что информация не подверглась несанкционированным изменениям, повреждениям или искажениям во время ее хранения, передачи или обработки. Защита целостности информации включает меры, направленные на предотвращение несанкционированных изменений данных и обнаружение возможных нарушений целостности.

Примеры целостности информации в правоохранительных органах включают следующее:

1. Цифровые доказательства, такие как фотографии, видео и звуковые записи, которые должны быть сохранены в неизменном виде для последующего использования в расследованиях.

2. Отчеты о преступлениях, свидетельства и другие документы, содержащие информацию, которая должна оставаться неприкосновенной и не подвергаться изменениям во избежание искажений фактов.

Доступность информации [25]:

Доступность информации относится к ее готовности и возможности быть полученной и использованной теми, кто имеет соответствующие права доступа. Она гарантирует, что информация доступна в нужное время и место, чтобы поддерживать эффективное функционирование правоохранительных органов и их оперативную деятельность. Защита доступности информации включает меры по обеспечению надежности и доступности информационных систем, предотвращению сбоев и обеспечению резервного копирования данных.

Примеры доступности информации в правоохранительных органах включают следующее:

1. Электронные базы данных, содержащие информацию о преступниках, уголовных делах и других данных, которые должны быть доступными сотрудникам органов внутренних дел для оперативного принятия решений.

2. Коммуникационные системы, такие как радиосвязь и системы передачи данных, которые обеспечивают связь, и обмен информацией между сотрудниками правоохранительных органов в режиме реального времени.

Основные аспекты кибербезопасности в правоохранительных органах включают:

1. Защиту информационных систем: Правоохранительные органы должны обеспечить надежную защиту своих информационных систем, включая компьютеры, серверы, сети и другое оборудование, от несанкционированного доступа, вредоносного программного обеспечения и других киберугроз.

2. Мониторинг и выявление инцидентов: Правоохранительные органы должны иметь системы мониторинга и обнаружения кибератак, чтобы оперативно реагировать на инциденты безопасности, идентифицировать

уязвимости и предотвращать угрозы.

3. Расследование киберпреступлений: Правоохранительные органы играют важную роль в расследовании и пресечении киберпреступлений, таких как хакерские атаки, мошенничество, кража личных данных и другие преступления, связанные с использованием информационных технологий.

4. Сотрудничество и обмен информацией: Правоохранительные органы активно сотрудничают на национальном и международном уровнях для обмена информацией о киберугрозах, таких как новые виды вредоносного ПО, методы атак и уязвимости, с целью обеспечения коллективной защиты и эффективного противодействия киберпреступности.

5. Обучение и повышение осведомленности: Правоохранительные органы проводят обучение своих сотрудников по вопросам кибербезопасности, чтобы повысить их навыки в области защиты информационных систем и эффективного реагирования на киберугрозы.

Примеры мер и технологий, используемых в кибербезопасности правоохранительных органов, включают системы защиты от DDoS-атак, брандмауэры, системы обнаружения вторжений (IDS/IPS), антивирусное программное обеспечение, шифрование данных и многое другое.

Важно отметить, что кибербезопасность в правоохранительных органах является непрерывным процессом, требующим постоянного обновления и совершенствования, так как угрозы и методы киберпреступности постоянно развиваются.

Кибератаки могут быть разнообразными и включать в себя следующие типы:

1. DDOS-атаки (атаки на отказ в обслуживании): При таких атаках злоумышленники создают огромное количество запросов к серверам или сетевым ресурсам с целью перегрузить их и привести к недоступности для законных пользователей.

2. Фишинг: Это метод мошенничества, при котором злоумышленники пытаются получить конфиденциальную информацию, такую как пароли или банковские данные, путем подделки электронных сообщений или веб-страниц.

3. Вредоносные программы (Malware): Это программы, разработанные с целью причинить вред информационным системам и получить несанкционированный доступ к данным. К таким программам относятся вирусы, трояны, шпионские программы и другие.

4. Атаки на слабые места в системе: Злоумышленники могут искать уязвимости в операционных системах, программном обеспечении или сетевых протоколах для получения несанкционированного доступа или выполнения вредоносных действий.

5. Социальная инженерия: Это метод манипулирования людьми с целью получения доступа к конфиденциальной информации или выполнения вредоносных действий. Злоумышленники могут использовать методы обмана, угроз или применять психологические техники для достижения своих целей.

Для защиты от кибератак в органах внутренних дел применяются различные меры кибербезопасности, включая установку защитного

программного обеспечения, мониторинг сетевой активности, обучение сотрудников правилам информационной безопасности и регулярное обновление систем и программного обеспечения.

Системы контроля и обнаружения вторжений для защиты информации и предотвращения кибератак.

Киберпреступники постоянно совершенствуют свои методы атак, поэтому необходимо применять эффективные системы контроля и обнаружения вторжений для предотвращения угроз и защиты национальной кибербезопасности.

Роль систем контроля и обнаружения вторжений в обеспечении безопасности информации:

Системы контроля и обнаружения вторжений (СКОВ) – это специализированные программные и аппаратные компоненты, предназначенные для мониторинга и анализа сетевой активности с целью обнаружения и предотвращения несанкционированного доступа к информационным системам. Они предоставляют возможность реагирования на потенциальные угрозы и предупреждения о возможных вторжениях.

Значение систем контроля и обнаружения вторжений:

— *Обнаружение угроз:* СКОВ помогают выявлять потенциальные угрозы и вторжения, позволяя оперативно принимать меры по предотвращению их негативных последствий.

— *Защита конфиденциальности:* СКОВ обеспечивают защиту конфиденциальных данных и информации, предотвращая несанкционированный доступ и утечку информации.

— *Снижение рисков:* СКОВ помогают уменьшить риски для информационных систем, предоставляя возможность оперативного реагирования на угрозы и восстановления после вторжений.

— *Соблюдение нормативных требований:* СКОВ помогают организациям и правоохранительным органам соблюдать требования законодательства в области информационной безопасности.

Примеры систем контроля и обнаружения вторжений:

— Фаерволы являются основным компонентом СКОВ и представляют собой программное или аппаратное оборудование, контролирующее трафик между сетями и применяющее правила фильтрации для предотвращения несанкционированного доступа. Они могут анализировать входящий и исходящий трафик, блокировать подозрительные соединения и обнаруживать атаки, такие как отказ в обслуживании (DDoS) или сканирование портов.

— Системы обнаружения вторжений (СОВ) предназначены для мониторинга и анализа сетевой активности с целью обнаружения аномального поведения и подозрительных событий. Они используют различные методы, включая сигнатурное обнаружение, поведенческий анализ и машинное обучение, чтобы выявлять атаки и аномалии в сети. Примером такой системы является Snort.

— Системы управления инцидентами (СУИ) предоставляют средства для регистрации, анализа и реагирования на инциденты информационной

безопасности. Они позволяют своевременное уведомление о нарушениях, сбор и анализ журналов событий, а также координацию и документирование действий по реагированию на инциденты. Примером такой системы является IBM QRadar.

— Системы защиты от вредоносных программ обнаруживают и блокируют вредоносные программы, такие как вирусы, троянские программы, шпионское ПО и рансомвары. Они используют сигнатуры и эвристический анализ для идентификации и блокировки вредоносных файлов и активности. Примерами таких систем являются McAfee, Kaspersky и Symantec.

Системы контроля и обнаружения вторжений играют важную роль в обеспечении безопасности информации в Республике Казахстан. Они помогают обнаруживать и предотвращать угрозы, защищать конфиденциальность данных, снижать риски и соблюдать нормативные требования. Приведенные примеры систем показывают, как различные технологии и подходы используются для обнаружения и защиты от кибератак. Однако, важно понимать, что безопасность информации требует комплексного подхода, который включает не только технические решения, но и обучение сотрудников, разработку политик безопасности и регулярное обновление систем.

Задачи и функции систем контроля и обнаружения вторжений включают следующие аспекты:

1. Обнаружение атак:

— Мониторинг сетевой активности для выявления подозрительных событий и аномалий.

— Анализ сигнатур атак и сравнение с известными шаблонами.

— Использование алгоритмов машинного обучения для обнаружения новых и неизвестных угроз.

2. Идентификация и аутентификация:

— Проверка подлинности пользователей и устройств для предотвращения несанкционированного доступа.

— Определение прав доступа и контроль привилегий пользователей.

3. Мониторинг и регистрация событий:

— Журналирование активности сети и системы для последующего анализа и отслеживания инцидентов.

— Анализ журналов событий с целью обнаружения необычной активности и аномалий.

4. Реагирование на инциденты:

— Оповещение и предупреждение о возможных инцидентах информационной безопасности.

— Автоматическая или полуавтоматическая реакция на угрозы, включая блокирование подозрительной активности или отключение уязвимых устройств.

5. Анализ и интеллектуальные функции:

— Использование алгоритмов машинного обучения для анализа данных и выявления скрытых связей и шаблонов.

— Предоставление статистических отчетов и аналитики о безопасности сети и системы.

6. Управление политиками безопасности:

— Конфигурирование и управление правилами и политиками безопасности сети и системы.

— Обновление и модификация правил в соответствии с новыми угрозами и требованиями безопасности.

7. Интеграция с другими системами:

— Взаимодействие и интеграция с другими системами безопасности, такими как системы защиты от вредоносных программ или системы управления инцидентами.

Основные компоненты систем контроля и обнаружения вторжений:

— Мониторинг сетевой активности: сбор, анализ и обработка данных о сетевом трафике для выявления подозрительной активности.

— Идентификация и аутентификация пользователей: использование методов и средств для проверки подлинности и идентификации пользователей сети.

— Обнаружение аномалий и атак: применение алгоритмов и технологий для обнаружения аномального поведения и попыток несанкционированного доступа.

— Журналирование и аудит: систематическое записывание событий и действий в сети для последующего анализа и исследования инцидентов.

Примеры систем контроля и обнаружения вторжений в Республике Казахстан:

—Центр обработки и анализа инцидентов в области безопасности информации (SOC-KZ): национальный центр, который отслеживает и реагирует на инциденты безопасности в киберпространстве.

—Система мониторинга и обнаружения вторжений «Astana-1»: разработана специально для защиты критической информационной инфраструктуры в Республике Казахстан.

—Использование систем SIEM (Security Information and Event Management): интегрированные системы, которые собирают, анализируют и реагируют на события безопасности в реальном времени.

Аналитические инструменты для мониторинга социальных сетей и интернета с целью выявления потенциальных угроз и предупреждения террористической и экстремистской деятельности.

В современном информационном обществе социальные сети и интернет играют значительную роль в обмене информацией, коммуникации и организации различных событий. Однако, среди этой свободы информации, могут присутствовать потенциальные угрозы безопасности, включая терроризм и экстремизм.

Аналитические инструменты для мониторинга социальных сетей:

Инструменты анализа текста: Алгоритмы и программы, которые позволяют анализировать текстовую информацию, выявлять ключевые слова,

выражения и контекст, связанный с потенциальной угрозой.

Машинное обучение и аналитика данных: Использование алгоритмов машинного обучения и анализа данных для обнаружения аномалий, выявления поведенческих паттернов и идентификации подозрительных активностей в социальных сетях.

Геолокационный анализ: Использование данных о местоположении пользователей социальных сетей для определения географического контекста и выявления потенциальных угроз в конкретных регионах.

Аналитические инструменты для мониторинга интернета:

Веб-сканирование и скрэпинг: Использование специальных программ для сканирования и сбора данных с веб-сайтов и интернет-форумов, связанных с террористической и экстремистской деятельностью.

Анализ социальных графов: Использование методов анализа социальных сетей для выявления связей и взаимодействий между потенциальными участниками террористических и экстремистских групп.

Анализ изображений и видео: Использование алгоритмов компьютерного зрения для обнаружения и анализа изображений и видео, связанных с потенциальной угрозой.

Примеры аналитических инструментов:

Palantir Gotham: Платформа для интеграции и анализа данных, используемая правоохранительными органами для выявления связей между лицами, местами и событиями.

Dataminr: Платформа мониторинга социальных медиа, которая использует алгоритмы машинного обучения для обнаружения потенциальных угроз и экстремистских сообщений.

Recorded Future: Инструмент анализа данных, который помогает правоохранительным органам прогнозировать и предотвращать кибератаки и террористические акты на основе анализа информации из различных источников.

Аналитические инструменты играют важную роль в обеспечении безопасности и предотвращении террористической и экстремистской деятельности. С помощью этих инструментов правоохранительные органы могут эффективно мониторить социальные сети и интернет, выявлять потенциальные угрозы и предпринимать соответствующие меры для их предотвращения. Примеры таких инструментов включают Palantir Gotham, Dataminr и Recorded Future. Эти инструменты помогают правоохранительным органам анализировать данные, выявлять связи и паттерны, а также прогнозировать возможные угрозы.

Системы идентификации и аутентификации для обеспечения безопасности доступа к информации и ресурсам.

В рамках работы правоохранительных органов особое внимание уделяется защите и конфиденциальности информации, поэтому системы идентификации и аутентификации являются неотъемлемой частью в обеспечении безопасности доступа к этой информации.

1. Идентификация:

Идентификация в органах внутренних дел РК представляет собой процесс определения личности или сущности, запрашивающей доступ к системе или ресурсам. Она осуществляется для установления легитимности пользователей и контроля доступа к информации.

Примеры систем идентификации: Логин и пароль, персональный идентификационный номер (ИИН), биометрическая идентификация (отпечатки пальцев, распознавание лица), удостоверения личности (служебные удостоверения), смарт-карты.

2. Аутентификация:

Аутентификация в органах внутренних дел РК является процессом проверки подлинности представленных идентификационных данных. Она осуществляется для обеспечения безопасности доступа к информации и ресурсам и предотвращения несанкционированного использования.

Примеры систем аутентификации: Парольная аутентификация (ввод пароля), биометрическая аутентификация (отпечатки пальцев, распознавание лица), двухфакторная аутентификация (пароль + одноразовый код), аутентификация на основе сертификатов.

3. Примеры систем и практическое применение:

Система учетных записей сотрудников: В органах внутренних дел РК используется система учетных записей для идентификации и аутентификации сотрудников. Каждому сотруднику присваивается уникальное имя пользователя и пароль, позволяющие им получать доступ к системам и информации в рамках своих полномочий.

Биометрическая аутентификация: Для повышения безопасности доступа к особым ресурсам и информации, органы внутренних дел РК могут использовать системы биометрической аутентификации, такие как сканеры отпечатков пальцев или системы распознавания лица. Это позволяет убедиться в подлинности пользователя на основе его уникальных физических характеристик.

Смарт-карты и сертификаты: Для обеспечения безопасности доступа к особым системам и ресурсам, органы внутренних дел РК могут использовать смарт-карты или сертификаты. Смарт-карта содержит зашифрованную информацию о пользователе, а сертификат является электронным документом, подтверждающим подлинность пользователя.

Двухфакторная аутентификация: Для повышения безопасности доступа к критической информации, органы внутренних дел РК могут применять двухфакторную аутентификацию. Например, сотрудник должен ввести пароль и предоставить одноразовый код, полученный через мобильное устройство или специальное устройство аутентификации.

Системы идентификации и аутентификации играют ключевую роль в обеспечении безопасности доступа к информации и ресурсам органов внутренних дел Республики Казахстан. Идентификация позволяет определить личность или сущность, а аутентификация проверяет подлинность представленных идентификационных данных. Примеры систем идентификации и аутентификации включают логин и пароль, биометрическую

аутентификацию, системы на основе смарт-карт и сертификатов. Применение этих систем позволяет эффективно защитить информацию и ресурсы органов внутренних дел РК от несанкционированного доступа и потенциальных угроз.

4. Роль информационных технологий в расследованиях преступлений.

Преступления – это деяния, которые признаются противозаконными и подлежат уголовной или административной ответственности в соответствии с законодательством Казахстана. Преступления характеризуются нарушением правил и норм, установленных законодательством, и причинением вреда обществу, частным лицам или государству.

В Казахстане преступления классифицируются на основе своей тяжести и характера на уголовные и административные преступления.

Уголовные преступления: Уголовные преступления являются наиболее серьезными правонарушениями и подлежат расследованию и судебному преследованию. Они включают преступления против жизни и здоровья, против имущества, против общественной безопасности и порядка, против общественной нравственности и другие. Уголовные преступления регулируются Уголовным кодексом РК.

Административные преступления: Административные преступления являются менее серьезными нарушениями, чем уголовные преступления. Они подлежат рассмотрению в административном порядке и влекут за собой применение административных наказаний, таких как штрафы, лишение прав или другие меры. Административные преступления могут включать нарушения в области дорожного движения, нарушения общественного порядка, административные нарушения в сфере экономики и другие. Административные преступления регулируются Кодексом Республики Казахстан об административных правонарушениях.

Преступления в РК являются серьезной проблемой, и правоохранительные органы стремятся предотвращать, раскрывать и пресекать преступную деятельность, обеспечивая безопасность общества и справедливость.

Форензические инструменты и методы анализа цифровых следов.

Форензические инструменты помогают выявлять и документировать преступления, анализируя цифровые следы на компьютерах, мобильных устройствах, цифровых камерах и других электронных устройствах.

Форензика (от лат. «forensis» - относящийся к суду) - наука о применении научных и технических методов для сбора, анализа и интерпретации доказательств с целью расследования преступлений и поддержки судебного процесса.

Значение форензики в правоохранительной деятельности:

- Обнаружение и раскрытие преступлений: форензические методы позволяют выявить, собрать и анализировать доказательства, необходимые для

раскрытия преступлений и идентификации виновных.

- Справедливость и судебный процесс: форензика обеспечивает представление надежных и достоверных доказательств, которые используются в судебных процессах для принятия справедливых решений.

Роль форензики в сборе доказательств:

- Следственный сбор: сбор физических следов, обнаружение и фиксация улик, таких как отпечатки пальцев, ДНК, следы обуви и другие.
- Цифровые следы: извлечение и анализ данных с цифровых устройств, таких как компьютеры, мобильные телефоны, планшеты и другие электронные устройства.

Форензический анализ и интерпретация доказательств:

- Баллистическая экспертиза: анализ огнестрельного оружия и пуль, определение их типа, калибра и места происхождения.
- Дактилоскопия: сравнение отпечатков пальцев для идентификации личности.
- Документальная экспертиза: исследование подлинности и подделки документов.
- Химический анализ: определение веществ, следов применения наркотиков, ядов и других веществ.

Форензика и использование современных технологий:

- Компьютерная форензика: извлечение и анализ данных с компьютеров, поиск удаленных файлов, анализ сетевой активности.
- Мобильная форензика: извлечение данных с мобильных устройств, включая сообщения, фотографии, видео и другие цифровые следы.
- Киберфорензика: исследование киберпреступлений, взломов, кражи данных и других компьютерных преступлений.

Примеры форензических инструментов и практический опыт:

1. Cellebrite UFED: инструмент для извлечения данных с мобильных устройств.

- Пример использования: извлечение сообщений и фотографий с мобильного устройства подозреваемого.

2. EnCase Forensic: программное обеспечение для анализа компьютерных данных.

- Пример использования: восстановление удаленных файлов с жесткого диска компьютера для обнаружения уничтоженных доказательств.

3. X-Ways Forensics: инструмент для обработки и анализа цифровых следов.

- Пример использования: анализ метаданных фотографий для определения места и времени совершения преступления.

Форензические инструменты и методы анализа цифровых следов играют важную роль в расследовании преступлений и обеспечении безопасности информации в органах внутренних дел Республики Казахстан. Они помогают выявлять, документировать и интерпретировать цифровые следы на компьютерах, мобильных устройствах, цифровых камерах и других электронных устройствах. Применение форензических инструментов позволяет

собирать надежные доказательства и способствует эффективности правоохранительных операций.

Использование специализированных баз данных и программных систем для сопоставления и анализа улик, поиска подозреваемых и установления связей между преступниками.

В рамках правоохранительной деятельности Республики Казахстан (РК) использование специализированных баз данных и программных систем является важным инструментом для эффективного сопоставления и анализа улик, поиска подозреваемых и установления связей между преступниками.

I. Роль специализированных баз данных и программных систем в правоохранительной деятельности РК:

- Сопоставление улик: системы баз данных позволяют хранить информацию о физических и цифровых уликах, таких как отпечатки пальцев, ДНК, баллистические данные и другие. Они помогают сопоставить найденные улики с записями, ранее зарегистрированными в базе данных, для идентификации подозреваемых или установления связей между различными преступлениями.
- Поиск подозреваемых: специализированные системы могут содержать информацию о преступниках, ранее судимых лицах, розыске и других данных, необходимых для поиска и идентификации подозреваемых в совершении преступлений. Это позволяет сократить время и усилия, затрачиваемые на поиск и расследование преступников.
- Установление связей: базы данных и программные системы также предоставляют возможность анализировать информацию о преступлениях и подозреваемых для выявления связей и сводок между различными случаями, преступными группировками или преступниками. Это помогает в построении обширной картины преступной деятельности и эффективной борьбе с преступностью.

II. Примеры специализированных баз данных и программных систем:

1. Единая база данных улик и ДНК: такая система позволяет хранить информацию о физических уликах, отпечатках пальцев, ДНК и других биологических материалах, найденных на местах преступлений. Система позволяет сопоставлять улики с данными о подозреваемых и идентифицировать преступников.
2. Системы автоматизированного розыска: такие системы содержат информацию о лицах, объявленных в розыск, лицах, находящихся под следствием, и других категориях подозреваемых. Они позволяют быстро и эффективно идентифицировать и локализовать подозреваемых.
3. Системы анализа связей: такие системы позволяют анализировать данные о преступлениях и подозреваемых для выявления связей и сводок. Например, они могут помочь определить связи между преступниками, членами преступных группировок или различными преступлениями, что способствует эффективному расследованию и предотвращению преступлений.

Использование специализированных баз данных и программных систем в органах внутренних дел РК играет важную роль в обеспечении безопасности и

эффективности правоохранительной деятельности. Они помогают сопоставлять улики, идентифицировать подозреваемых и устанавливать связи между преступниками. Примеры таких систем включают единую базу данных улик и ДНК, системы автоматизированного розыска и системы анализа связей. Эти инструменты способствуют более эффективному расследованию и предотвращению преступлений, обеспечивая безопасность в Республике Казахстан.

Компьютерное моделирование и симуляция для воссоздания преступных событий и определения их деталей.

В современной правоохранительной деятельности Республики Казахстан (РК) компьютерное моделирование и симуляции играют важную роль в воссоздании преступных событий и определении их деталей. Эти технологии позволяют правоохранительным органам более точно понять динамику преступных событий, их возможные последствия и развитие событий.

I. Роль компьютерного моделирования и симуляций в правоохранительной деятельности:

- Воссоздание преступных событий: компьютерное моделирование позволяет создать виртуальную среду, в которой возможно воссоздать преступные события с использованием доступной информации, фактов и свидетельских показаний. Это позволяет получить более полное представление о происходивших событиях и определить их детали.
- Анализ динамики преступлений: с помощью компьютерных моделей и симуляций можно анализировать динамику преступлений и их развитие. Это позволяет правоохранительным органам предсказывать возможные сценарии и последствия преступных действий, что помогает принимать эффективные меры по предотвращению и борьбе с преступностью.
- Обучение и тренировка: компьютерные модели и симуляции используются для обучения и тренировки правоохранительных сотрудников. Виртуальные среды позволяют проводить тренировочные сценарии, имитирующие реальные преступные ситуации, и позволяют сотрудникам развивать навыки реагирования и принятия решений.

II. Примеры использования компьютерного моделирования и симуляций:

1. Моделирование преступлений на местах происшествий: с помощью компьютерных моделей можно воссоздать место преступления и провести виртуальное расследование. Это позволяет определить возможные версии происшествия, взаимодействие объектов и лиц, а также получить дополнительные детали и улики.

2. Симуляция террористических актов: компьютерные симуляции позволяют проводить тренировки и сценарии для предотвращения террористических актов. Виртуальные среды позволяют проверить эффективность тактик и мер безопасности, а также разрабатывать стратегии по борьбе с терроризмом.

3. Моделирование распространения преступности: компьютерные модели позволяют анализировать данные о преступности и прогнозировать ее распространение в разных регионах. Это помогает правоохранительным

органам выявить «горячие точки» преступности и принять меры для их предотвращения.

Компьютерное моделирование и симуляции играют важную роль в правоохранительной деятельности РК. Они помогают воссоздать преступные события, анализировать динамику преступлений, обучать и тренировать сотрудников и принимать эффективные меры по предотвращению и борьбе с преступностью. Примеры использования этих технологий включают моделирование преступлений на местах происшествий, симуляцию террористических актов и моделирование распространения преступности.

Вопросы и задания для самоконтроля:

1. *Задание №1:* Вы являетесь руководителем отдела. Вам поручено провести презентацию для сотрудников, в которой Вы должны дать определение информационных технологий и объяснить их значение для эффективного функционирования органов внутренних дел. Подготовьте краткое выступление и обоснуйте важность информационных технологий в Вашей работе.

2. *Задание №2:* Вы работаете в отделе оперативного розыска и Вам поступило задание разработать рекомендации по использованию информационных технологий для усиления оперативно-розыскной деятельности, обеспечения безопасности и содействия в расследованиях преступлений. Составьте список конкретных мер и технологий, которые Вы рекомендуете внедрить и объясните, как они могут улучшить работу Вашего отдела.

3. *Задание №3:* Ваш отдел столкнулся с серьезным нарушением информационной безопасности. Вам поручено провести анализ текущей системы безопасности и предложить меры по улучшению с использованием информационных технологий. Опишите основные уязвимости в системе безопасности, рекомендуйте соответствующие технологические решения и обоснуйте их выбор.

4. *Задание №4:* Ваш отдел получил сложное дело, требующее детального анализа большого объема информации. Вам поручено использовать информационные технологии для эффективного расследования. Опишите, какие технологические инструменты и базы данных Вы будете использовать для сбора, анализа и хранения данных, а также объясните, как эти технологии помогут ускорить и улучшить процесс расследования.

5. Что представляют собой информационные технологии?

6. Какое значение имеют информационные технологии для органов внутренних дел?

7. Какие основные компоненты включают в себя информационные технологии в контексте правоохранительных органов?

8. Как информационные технологии способствуют эффективному функционированию органов внутренних дел?

9. Как информационные технологии усиливают оперативно-розыскную деятельность органов внутренних дел?

10. Какие инструменты и технологии используются в рамках информационных технологий для обеспечения безопасности?

11. Как информационные технологии способствуют содействию в расследованиях преступлений?

12. Приведите примеры конкретных информационных технологий, которые используются в оперативно-розыскной деятельности и расследованиях преступлений.

13. Как информационные технологии способствуют обеспечению безопасности в органах внутренних дел?

14. Какие меры безопасности можно реализовать с помощью информационных технологий?

15. Какие типы угроз безопасности могут быть предотвращены с помощью информационных технологий?

16. Как информационные технологии помогают в обнаружении и анализе потенциальных угроз безопасности?

17. Как информационные технологии способствуют расследованиям преступлений?

18. Какие методы и технологии используются для сбора, анализа и обработки данных в рамках расследований преступлений?

19. Как информационные технологии способствуют идентификации и локализации преступных действий?

20. Какие преимущества и ограничения существуют при использовании информационных технологий в расследованиях преступлений?

Список литературы

1. Конституция Республики Казахстан от 30 августа 1995 года (с изменениями и дополнениями от 01.01.2023 г.).

2. О национальной безопасности: Закон Республики Казахстан от 6 января 2012 года (с изменениями и дополнениями от 26.02.2023).

3. Об информатизации: Закон Республики Казахстан от 24 ноября 2015 года (с изменениями и дополнениями от 19.04.2023).

4. Об электронном документе и электронной цифровой подписи: Закон РК от 7 января 2003 г. № 370-II // Каз. правда. - 2003. - 10 янв. (с изменениями и дополнениями от 19.04.2023г.).

5. Алпеев А.С. Терминология безопасности: кибербезопасность, информационная безопасность. // Вопросы кибербезопасности. – 2014. - 5 (8).

6. Федотов Н.Н. Форензика-компьютерная криминалистика. - Москва, 2007.;

7. Безкоровайный М.М., Татузов А.Л. Кибербезопасность подходы к определению понятия. // Вопросы кибербезопасности. – 2014. - 1 (2).

8. Бураева Л.А. О некоторых вопросах обеспечения кибербезопасности в современных условиях. // Теория и практика общественного развития. – 2015. - 13.

9. Галатенко ВА. Основы информационной безопасности. Интернет-Университет Информационных Технологий (ИНТУИТ), 2008.

10. Карасев П.А. Политика безопасности США в глобальном информационном пространстве. – Москва, 2015.

11. Старовойтов А.В. Кибербезопасность как актуальная проблема современности. // Информатизация и связь. – 2011. – 6. – С. 4-7.

12. Сырбу А.В. Процессуальный порядок получения и использования информации с технических каналов связи в уголовном судопроизводстве: дис. канд. юрид. наук. — Караганда, 2005.

13. Анин Б.Ю. Защита компьютерной информации. — СПб.: БХВ-Петербург, 2000. - 384 с.

14. Компьютерное проникновение или заговор // Форпост. - 2002. - 4 июня.

15. Нугманова А.Т. (Завотпаева А.Т.) Частная жизнь граждан под наблюдением высоких технологий // Вестник Университета им. Д. Кунаева. — 2005. — № 2(15).

16. Преступления в сфере компьютерной информации: квалификация и доказывание: учеб. пособие / под ред. Ю.В. Гаврилина. - М.: ЮИ МВД РФ, 2003.

17. Гаврилин Ю.В. Расследование неправомерного доступа к компьютерной информации. - М., 2001.

18. Вечерский Д.А Шалькевич И.И. Расследование компьютерных преступлений. – Минск, 2001.

19. Нугманова А.Т. (Завотпаева А.Т.) Общие требования при реализации ОРМ на сетях телекоммуникаций // Информационно-коммуникационные технологии как основной фактор развития инновационного общества: мат-лы Международ. науч.практ. конф. - Усть-Каменогорск, 2007.

20. Комиссаров В., Гаврилов М., Иванов А. Обыск с извлечением компьютерной и информации. // Законность. - 1999. - № 3. – С. 90.

21. Information Technology for Management: Advancing Sustainable Profitable Business Growth, 10th Edition International Student Version / Efraim Turban, Carol Pollard, Gregory Wood / ISBN: 978-1-118-95895-7 July 2015, 392p.

22. Managing and Using Information Systems: A Strategic Approach by Keri E. Pearlson, Carol S. Saunders / 2019 /368 p.

23. Information Systems: A Manager's Guide to Harnessing Technology by John Gallaugher / Publisher: FlatWorld; 7th edition (January 1, 2018).

24. Cybercrime and Digital Forensics: An Introduction by Thomas J. Holt, Adam M. Bossler, Kathryn C. Seigfried-Spellar / Copyright 2022 / ISBN 9780367360078 / 812 Pages 33 B/W Illustrations / Published May 31, 2022 by Routledge.

ТЕМА 2. ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

Цель: изучить применение информационных технологий в органах внутренних дел с целью повышения эффективности правоохранительной деятельности, улучшения оперативности работы и обеспечения безопасности граждан и общества.

План:

1. Основные цели применения информационных технологий в ОВД.
2. Использование баз данных и информационных систем для хранения и обработки информации о преступлениях, преступниках и жертвах.
3. Электронное ведение учета и оперативный доступ к данным, включая паспортные и водительские удостоверения, информацию о судимости и другие важные документы.
4. Создание и поддержка сетей связи для оперативного обмена информацией между отделениями и подразделениями ОВД.
5. Основные принципы создания и поддержки сетей связи

1. Основные цели применения информационных технологий в ОВД.

Информационные технологии играют важную роль в работе органов внутренних дел Республики Казахстан. Они помогают автоматизировать и оптимизировать процессы, улучшают оперативность и эффективность работы правоохранительных органов, а также обеспечивают безопасность и надежность хранения и обработки информации.

Цель применения информационных технологий в органах внутренних дел заключается в обеспечении более эффективной, оперативной и безопасной работы правоохранительных органов.

IT используются для автоматизации процессов, хранения и обработки информации, обеспечения связи и обмена данными, анализа и выявления преступных событий, идентификации подозреваемых, предупреждения преступлений и террористической деятельности, а также для расследования и судебного преследования преступлений.

Основные цели применения информационных технологий в органах внутренних дел включают:

1. Улучшение оперативности и эффективности работы: Информационные технологии помогают автоматизировать рутинные процессы, ускоряют обработку информации и обмен данных, а также позволяют быстро находить и анализировать информацию, необходимую для оперативно-розыскной деятельности.

2. Обеспечение безопасности информации: Информационные технологии предоставляют механизмы для защиты информации от несанкционированного

доступа, включая шифрование, аутентификацию, контроль доступа и системы обнаружения вторжений.

3. Улучшение качества и достоверности доказательств: Использование специализированных программных средств и баз данных позволяет проводить анализ и сопоставление улик, идентифицировать связи между преступниками и их деятельностью, а также обеспечивает точность и надежность документации и представления доказательств в суде.

4. Предотвращение преступлений и борьба с терроризмом: Информационные технологии используются для мониторинга социальных сетей и интернета, выявления потенциальных угроз и предупреждения террористической и экстремистской деятельности.

5. Усиление сотрудничества и обмена информацией: Информационные технологии позволяют устанавливать эффективный обмен информацией между различными структурами правоохранительных органов, а также с международными партнерами, что способствует совместной борьбе с преступностью и транснациональными преступлениями.

Применение информационных технологий в ОВД РК направлено на повышение уровня безопасности граждан, обеспечение правопорядка и эффективной борьбы с преступностью.

2. Использование баз данных и информационных систем для хранения и обработки информации о преступлениях, преступниках и жертвах.

Использование баз данных и информационных систем для хранения и обработки информации о преступлениях, преступниках и жертвах в Республике Казахстан имеет ключевое значение для правоохранительных органов. Эти системы позволяют эффективно управлять и анализировать данные, связанные с преступлениями, и обеспечивают централизованное хранение информации для более эффективного расследования и предотвращения преступлений.

Одной из важных информационных систем, используемых в органах внутренних дел РК, является автоматизированная информационная система Единая база данных ОВД. Эта система объединяет информацию о преступлениях, преступниках, уликах, розыске и других аспектах оперативно-розыскной деятельности. В ней содержатся данные о ранее совершенных преступлениях, подозреваемых лицах, их личных данных, местах работы и проживания, а также информация о потерпевших и свидетелях. Система позволяет оперативно получать и обрабатывать данные, осуществлять поиск по различным критериям и проводить анализ связей между преступниками и их деятельностью.

Также, в органах внутренних дел РК используются специализированные базы данных, которые содержат информацию о преступлениях определенных видов, например, база данных о наркотической преступности, база данных о преступлениях экономической сферы и т. д. Эти базы данных позволяют

проводить анализ и мониторинг определенных видов преступности, выявлять тенденции и осуществлять превентивные меры.

Примером применения информационных систем и баз данных в органах внутренних дел РК является система Электронное следствие. Эта система предназначена для электронного ведения уголовных дел, автоматизации процессов расследования и судебного процесса. В ней хранятся материалы уголовных дел, судебные решения, протоколы допросов, экспертные заключения и другая важная информация. Система обеспечивает быстрый доступ к данным, позволяет проводить анализ и сверку информации, упрощает взаимодействие между сотрудниками правоохранительных органов и другими участниками уголовного процесса.

Использование баз данных и информационных систем в органах внутренних дел РК позволяет сократить время и усилия, затрачиваемые на обработку информации о преступлениях, улучшить качество анализа и оперативности реагирования на преступные события. Это способствует более эффективной борьбе с преступностью и обеспечению безопасности граждан Республики Казахстан.

3. Электронное ведение учета и оперативный доступ к данным, включая паспортные и водительские удостоверения, информацию о судимости и другие важные документы.

В современном информационном обществе электронные технологии играют все более важную роль в обеспечении эффективности работы правоохранительных органов. Одной из сфер, где применение информационных технологий имеет особое значение, является электронное ведение учета и оперативный доступ к данным. В Республике Казахстан такие системы активно применяются для учета различных документов, таких как паспортные и водительские удостоверения, информации о судимости и других важных документов.

Электронное ведение учета документов:

В Республике Казахстан введены электронные системы учета паспортных и водительских удостоверений. Это позволяет упростить и ускорить процедуру оформления документов, а также обеспечить их надежное хранение и доступность.

Система Единая база данных паспортов предоставляет возможность быстрого доступа к информации о гражданах, включая данные о регистрации, смене места жительства и других изменениях.

Аналогично, электронное ведение учета водительских удостоверений позволяет оперативно получать информацию о водителях, их правах и нарушениях.

Преимущества электронного ведения учета включают централизованное хранение данных, возможность оперативного обновления информации и легкий доступ к ней со стороны соответствующих органов.

Информация о судимости:

В Республике Казахстан ведется электронный учет данных о судимости граждан. Это позволяет быстро получать информацию о судимости лиц при необходимости, упрощает процесс проверки ранее совершенных преступлений и облегчает расследование преступлений.

Электронный учет информации о судимости также способствует повышению безопасности, так как позволяет выявлять рецидивистов и принимать меры по их наблюдению и контролю.

Другие важные документы и данные:

Кроме паспортных и водительских удостоверений, электронные системы также используются для учета и хранения других важных документов, таких как данные о регистрации юридических лиц, справки о наличии или отсутствии задолженности перед государством и другие.

Примером такой системы является Единая информационная система учета задолженности перед государством, которая позволяет оперативно получать информацию о задолженности организаций и физических лиц перед налоговыми и другими государственными органами.

Применение информационных технологий в электронном ведении учета и оперативном доступе к данным в органах внутренних дел Республики Казахстан имеет существенное значение для обеспечения безопасности и эффективности правоохранительной деятельности. Это позволяет оперативно получать и обрабатывать информацию о преступлениях, преступниках и других важных данных, способствуя более эффективной борьбе с преступностью и обеспечению правопорядка в стране.

4. Создание и поддержка сетей связи для оперативного обмена информацией между отделениями и подразделениями ОВД.

В современном информационном обществе связь и обмен информацией играют ключевую роль в обеспечении эффективной работы правоохранительных органов.

Введение в сети связи в органах внутренних дел

Сети связи – это инфраструктура и технологии, которые обеспечивают передачу информации между различными узлами и устройствами.

Сети связи могут быть проводными или беспроводными, локальными или глобальными, и они основаны на различных протоколах и стандартах связи.

Роль сетей связи в оперативной деятельности органов внутренних дел

- Обмен информацией: Сети связи обеспечивают оперативный обмен информацией между отделениями и подразделениями, позволяя передавать важные данные о преступлениях, розыске, происшествиях и других событиях.
- Координация действий: Сети связи позволяют правоохранительным органам координировать свои действия и оперативно реагировать на происшествия, обмениваясь информацией и инструкциями.
- Взаимодействие и сотрудничество: Сети связи способствуют усилению

взаимодействия и сотрудничества между различными подразделениями органов внутренних дел, что повышает эффективность и оперативность их работы.

Использование сетей связи в органах внутренних дел Республики Казахстан

Локальные сети (LAN) в отделениях и подразделениях

- Кабельная и беспроводная организация сети.
- Установка и настройка сетевого оборудования, такого как коммутаторы, маршрутизаторы и пр.
- Локальные сети обеспечивают оперативный обмен информацией и доступ к общим ресурсам в пределах отдельных отделений и подразделений.

Глобальные сети (WAN) для взаимодействия между отделениями

- Виртуальные частные сети (VPN) для защищенного обмена информацией между удаленными отделениями и подразделениями.
- Использование специализированных сетей связи, таких как сеть спецслужб или внутренних коммуникаций, для оперативного взаимодействия между отделениями.

Безопасность сетей связи

- Защита сетей связи от несанкционированного доступа и кибератак
- Использование систем защиты, шифрования и аутентификации для обеспечения безопасности данных и связи.

Примеры использования сетей связи в органах внутренних дел Республики Казахстан:

- Установка локальных сетей в полицейских участках, позволяющих оперативно обмениваться информацией о происшествиях и розыске.
- Использование глобальных сетей для связи между отделениями и центральными органами внутренних дел, обеспечивая оперативное реагирование на происшествия и скоординированную работу.
- Внедрение систем виртуальных частных сетей (VPN) для защищенного обмена информацией между удаленными подразделениями органов внутренних дел.
- Создание специализированных сетей связи, таких как сеть спецслужб, для оперативного обмена информацией с другими правоохранительными органами.

Сети связи играют важную роль в оперативной деятельности органов внутренних дел Республики Казахстан. Они обеспечивают эффективное взаимодействие и оперативный обмен информацией между отделениями и подразделениями, способствуя координации действий и повышению безопасности. Применение современных информационных технологий и развитие сетей связи являются неотъемлемой частью современной правоохранительной деятельности в Республике Казахстан.

Значение сетей связи в органах внутренних дел

Сети связи играют важную роль в оперативно-розыскной деятельности органов внутренних дел Республики Казахстан. Они обеспечивают эффективный обмен информацией, оперативный доступ к данным, координацию действий и оперативное реагирование на происшествия.

1. Обмен информацией и оперативный доступ к данным: Сети связи позволяют осуществлять быстрый и безопасный обмен информацией между отделениями и подразделениями ОВД. Это включает передачу оперативных данных, информации о происшествиях, розыске и других сведений, необходимых для оперативно-розыскной работы. Применение сетей связи обеспечивает быстрый доступ к цифровым базам данных, электронным документам, позволяет оперативно получать информацию о гражданах, судимости, транспортных средствах и других объектах интереса.

Примеры:

- Использование специализированных информационных систем и баз данных для хранения и обработки информации о преступлениях, преступниках и жертвах. Сети связи обеспечивают доступ к этой информации для оперативных служб ОВД и позволяют оперативно извлекать необходимые данные для расследования преступлений.
- Электронное ведение учета и оперативный доступ к данным, включая паспортные и водительские удостоверения, информацию о судимости и другие важные документы. Сети связи обеспечивают быстрый доступ к электронным базам данных, что позволяет оперативным сотрудникам получать необходимые сведения о гражданах в режиме реального времени.

2. Координация действий и оперативное реагирование на происшествия: Сети связи позволяют эффективно координировать действия между различными отделениями и подразделениями ОВД. Они обеспечивают оперативное обмен информацией о происшествиях, координацию оперативных мероприятий и оперативное реагирование на происшествия различного характера.

3. Использование радиосвязи и систем передачи данных для оперативной связи между сотрудниками ОВД на местах происшествий. Это позволяет оперативно передавать информацию о происшествиях, принимать оперативные решения и координировать действия служб безопасности.

4. Использование систем видеонаблюдения и передачи видеоданных для оперативного контроля обстановки и быстрого реагирования на происшествия. Видеокамеры, установленные на общественных местах или важных объектах, передают видеоинформацию в реальном времени, позволяя оперативным службам получать актуальные данные и оперативно реагировать на происшествия.

5. Усиление взаимодействия между отделениями и подразделениями: Сети связи способствуют усилению взаимодействия и сотрудничества между различными отделениями и подразделениями ОВД. Они обеспечивают оперативный обмен информацией, координацию оперативных мероприятий, планирование и совместную работу.

6. Использование электронных платформ и систем управления кейсами для совместной работы и обмена информацией между следователями, оперативными сотрудниками и другими специалистами. Это позволяет эффективно расследовать преступления, собирать доказательства и обмениваться необходимой информацией.

7. Использование электронных систем планирования и учета оперативных мероприятий. Сети связи обеспечивают оперативное информирование и координацию действий между различными службами ОВД, позволяют эффективно планировать и контролировать оперативные мероприятия.

Использование сетей связи в органах внутренних дел РК имеет огромное значение для обеспечения оперативной деятельности, обмена информацией, координации действий и усиления взаимодействия между отделениями и подразделениями. Применение современных информационных технологий и развитие сетей связи способствуют повышению эффективности правоохранительной деятельности и обеспечению безопасности в Республике Казахстан.

5. Основные принципы создания и поддержки сетей связи.

Инфраструктура сетей связи

Для обеспечения эффективного функционирования информационной системы ОВД, необходима надежная и безопасная инфраструктура сетей связи.

1) Выбор подходящих технологий и оборудования:

- Определение требований: Первоначальный шаг заключается в определении требований сетевой инфраструктуры, учитывая особенности деятельности ОВД. Необходимо учесть объем передаваемой информации, необходимость мобильной связи, требования к скорости и надежности передачи данных и другие факторы.
- Выбор подходящих технологий: На основе определенных требований необходимо выбрать соответствующие технологии, такие как проводные и беспроводные сети связи, цифровые системы передачи данных, IP-телефония и др.
- Выбор оборудования: После определения технологий необходимо выбрать соответствующее сетевое оборудование, включая коммутационные устройства, маршрутизаторы, беспроводные точки доступа, серверы и другое оборудование, соответствующее требованиям и задачам ОВД.

2. Развертывание сетевой инфраструктуры:

- Кабельная проводка: Надлежащая кабельная проводка является основой надежной сетевой инфраструктуры. Необходимо проектировать и устанавливать кабельные системы, включая витую пару, оптоволокно и коаксиальные кабели, с учетом требований к пропускной способности и дальности передачи сигнала.
- Коммутационное оборудование: Коммутационное оборудование играет ключевую роль в управлении трафиком в сети. Оно обеспечивает соединение между устройствами и передачу данных. Важно выбрать подходящие коммутаторы, маршрутизаторы и другое коммутационное оборудование, учитывая объем трафика и требования безопасности.
- Беспроводные сети: В некоторых случаях необходимо развернуть

беспроводные сети связи для обеспечения мобильности сотрудников ОВД. Важно правильно настроить беспроводные точки доступа, обеспечивая безопасное подключение и эффективное покрытие сигнала.

3. Обеспечение надежности и безопасности сетей связи:

- Резервирование сетевых элементов: Для обеспечения надежности сетевой инфраструктуры рекомендуется использовать резервирование сетевых элементов. Например, дублирование коммутационного оборудования, настройка резервных каналов связи и использование резервных источников питания.
- Межсетевые экраны и системы защиты: Для обеспечения безопасности сетей связи необходимо использовать межсетевые экраны (firewalls) и другие системы защиты, которые могут контролировать и фильтровать трафик, а также обнаруживать и предотвращать несанкционированный доступ.
- Шифрование данных: Важно использовать методы шифрования данных при передаче конфиденциальной информации по сети, чтобы обеспечить ее конфиденциальность и предотвратить несанкционированный доступ.

Примеры:

1. Внедрение оптоволоконной сети: Органы внутренних дел РК могут решить развернуть оптоволоконную сеть для быстрой передачи данных между отделениями и подразделениями. Это обеспечит высокую пропускную способность, надежность и безопасность передачи информации.
2. Использование IP-телефонии: ОВД может внедрить систему IP-телефонии, позволяющую сотрудникам осуществлять голосовую связь через сеть данных. Это облегчит внутреннюю коммуникацию и снизит затраты на связь.
3. Резервирование коммутационного оборудования: Для обеспечения непрерывности работы сети органы внутренних дел могут установить дублирующее коммутационное оборудование и настроить его на автоматическое переключение в случае сбоя или отказа основного оборудования.

Инфраструктура сетей связи играет важную роль в оперативной деятельности органов внутренних дел Республики Казахстан. Правильный выбор технологий и оборудования, развертывание сетевой инфраструктуры и обеспечение надежности и безопасности являются ключевыми аспектами в создании эффективной сети связи. Приведенные примеры демонстрируют практическое применение информационных технологий в органах внутренних дел РК для повышения оперативности, эффективности и безопасности их деятельности.

Протоколы и стандарты связи

Для обеспечения эффективной и безопасной связи используются протоколы и стандарты связи.

Основные протоколы связи

1. TCP/IP:

- TCP/IP (Transmission Control Protocol/Internet Protocol) является основным протоколом связи в интернете. Он обеспечивает надежную доставку

данных, разбивая их на пакеты и устанавливая соединение между отправителем и получателем. TCP/IP является стандартом сетевого протокола, который позволяет различным устройствам взаимодействовать и обмениваться информацией в сети.

2. Ethernet:

- Ethernet является технологией сетевой связи, которая используется для подключения устройств в локальных сетях (LAN). Она определяет способы передачи данных по физическому соединению, используя специальные кабели и сетевое оборудование, такое как коммутаторы и маршрутизаторы. Ethernet является широко распространенным протоколом связи и обеспечивает высокую пропускную способность и скорость передачи данных.

Стандарты безопасности и защиты данных в РК:

1. Законодательство РК:

- В Республике Казахстан действует законодательство, которое регулирует вопросы безопасности и защиты данных. Закон РК «О персональных данных» и другие законы и нормативные акты устанавливают правила обработки, хранения и защиты персональных данных граждан.

2. Стандарты безопасности информации:

- В органах внутренних дел РК применяются различные стандарты безопасности информации, такие как ISO/IEC 27001. Эти стандарты определяют требования к системам управления информационной безопасностью и организационным мерам по защите данных.

3. Криптография:

- Криптография играет важную роль в обеспечении защиты данных. В РК используются различные криптографические алгоритмы и протоколы для шифрования и обеспечения конфиденциальности данных, такие как AES (Advanced Encryption Standard) и SSL/TLS (Secure Sockets Layer/Transport Layer Security).

В органах внутренних дел РК применяются протоколы TCP/IP и Ethernet для обеспечения связи и обмена информацией между отделениями и подразделениями. Например, полицейские автомобили могут быть оборудованы системами связи на базе протокола TCP/IP, которые позволяют им оперативно получать информацию о происшествиях, проверять данные и координировать свои действия.

- Для защиты данных в органах внутренних дел РК применяются стандарты безопасности информации, такие как ISO/IEC 27001. Например, базы данных с информацией о преступлениях, преступниках и жертвах могут быть защищены с использованием соответствующих мер безопасности, таких как контроль доступа, шифрование данных и резервное копирование.
- Криптография применяется для защиты конфиденциальности данных в органах внутренних дел РК. Например, при передаче секретной информации между подразделениями или при использовании электронной почты для обмена конфиденциальными документами может быть применено шифрование с использованием современных криптографических алгоритмов.

Протоколы и стандарты связи играют важную роль в оперативной

деятельности органов внутренних дел Республики Казахстан. Они обеспечивают эффективный обмен информацией, координацию действий и оперативное реагирование на происшествия. Стандарты безопасности и защиты данных гарантируют сохранность и конфиденциальность информации. Приведенные примеры демонстрируют практическое применение информационных технологий и стандартов в органах внутренних дел РК.

Управление и мониторинг сетей связи

Эффективное управление и мониторинг этих сетей играют важную роль в обеспечении надежной и безопасной связи, обмена информацией и оперативного реагирования на происшествия. В данной лекции мы рассмотрим основные аспекты управления и мониторинга сетей связи в органах внутренних дел РК, а именно: администрирование сетевых ресурсов, мониторинг и диагностика сети, а также резервное копирование и восстановление данных.

1. ***Администрирование сетевых ресурсов:***

- Администрирование сетевых ресурсов включает управление и контроль над сетевыми устройствами, сервисами и приложениями. Оно включает в себя настройку и конфигурирование сетевого оборудования, управление пользователями и правами доступа, а также мониторинг использования сетевых ресурсов.
- В органах внутренних дел РК администрирование сетевых ресурсов осуществляется специалистами по информационным технологиям, которые отвечают за обеспечение надежной и безопасной работы сети. Они выполняют установку и настройку сетевого оборудования, обновление программного обеспечения, создание и управление аккаунтами пользователей, а также контролируют доступ к сетевым ресурсам.

2. ***Мониторинг и диагностика сети:***

- Мониторинг и диагностика сети позволяют отслеживать состояние и производительность сетевых компонентов, обнаруживать возможные проблемы и неполадки, а также предотвращать и решать сетевые сбои. Это включает контроль доступности сетевых устройств, измерение пропускной способности, мониторинг сетевого трафика и анализ сетевых данных.
- В органах внутренних дел РК мониторинг и диагностика сети выполняются с помощью специализированных программных и аппаратных средств. Они позволяют оперативно выявлять проблемы в сети, анализировать трафик, контролировать загрузку сетевых устройств и принимать меры по их оптимизации.

3. ***Резервное копирование и восстановление данных:***

- Резервное копирование данных является важной составляющей управления сетью связи. Это процесс создания резервных копий информации, хранящейся на сетевых устройствах, с целью ее сохранения и возможности восстановления в случае потери или повреждения данных. Восстановление данных включает процедуры восстановления резервных копий и восстановление работы сетевых устройств.
- В органах внутренних дел РК резервное копирование и восстановление данных осуществляется с использованием специализированных

программных средств и систем хранения данных. Это позволяет обеспечить надежность и безопасность данных, а также быстрое восстановление работы сетевых устройств после возможных сбоев или инцидентов.

Примеры:

1. Администрирование сетевых ресурсов: Специалисты по информационным технологиям органов внутренних дел РК настраивают и обслуживают сетевое оборудование, такое как маршрутизаторы, коммутаторы, брандмауэры. Они также управляют пользователями и правами доступа к сетевым ресурсам, обеспечивая безопасность и конфиденциальность информации.

2. Мониторинг и диагностика сети: Системы мониторинга сети в органах внутренних дел РК позволяют контролировать доступность сетевых устройств, анализировать трафик, определять причины сетевых сбоев и предупреждать о возможных угрозах. Это помогает оперативно реагировать на проблемы и поддерживать надежность работы сети.

3. Резервное копирование и восстановление данных: В органах внутренних дел РК выполняется регулярное резервное копирование данных, хранящихся на серверах и других сетевых устройствах. Это позволяет защитить информацию от потери и восстановить ее в случае необходимости. Программные средства автоматического резервного копирования и системы хранения данных обеспечивают сохранность информации и быстрое восстановление работы сети.

Управление и мониторинг сетей связи в органах внутренних дел Республики Казахстан играют важную роль в обеспечении эффективной и безопасной связи, оперативного обмена информацией и координации действий. Администрирование сетевых ресурсов, мониторинг и диагностика сети, а также резервное копирование и восстановление данных являются неотъемлемой частью управления сетью связи. Благодаря применению соответствующих технологий и методов, органы внутренних дел РК могут обеспечить надежность, безопасность и оперативность своей сетевой инфраструктуры.

Системы коммуникации для оперативного обмена информацией

Для эффективного обмена информацией используются специальные системы коммуникации, которые обеспечивают быструю передачу данных, сохранность информации и конфиденциальность обмена.

Системы коммуникации – это комплекс технических средств и программного обеспечения, предназначенных для обмена информацией между различными узлами или участниками сети.

В контексте органов внутренних дел РК, системы коммуникации используются для оперативного обмена информацией между отделениями, подразделениями, полицейскими и другими участниками оперативной деятельности.

Основные принципы работы систем коммуникации:

1. Быстрота передачи данных: Оперативный обмен информацией требует высокой скорости передачи данных между участниками. Системы

коммуникации должны обеспечивать быструю и надежную передачу данных, чтобы оперативные события и инструкции могли быть распространены в кратчайшие сроки.

2. Конфиденциальность и безопасность: В оперативной деятельности органов внутренних дел РК обмен информацией может содержать конфиденциальную и чувствительную информацию. Системы коммуникации должны обеспечивать защиту информации от несанкционированного доступа и поддерживать соответствующие меры безопасности, такие как шифрование и аутентификация.

3. Надежность и доступность: Системы коммуникации должны быть надежными и доступными для использования в любое время. Оперативные события могут происходить в любой момент, поэтому системы коммуникации должны быть готовы к непрерывной работе и обеспечивать доступность информации для участников оперативной деятельности.

Системы коммуникации для оперативного обмена информацией играют ключевую роль в деятельности органов внутренних дел Республики Казахстан. Они обеспечивают быструю передачу данных, конфиденциальность и безопасность обмена, а также надежность и доступность системы. Примерами систем коммуникации являются радиосвязь, системы передачи данных и системы видеонаблюдения.

Вопросы и задания для самоконтроля:

1. *Задача:* В вашем отделе введена система электронного ведения учета. Опишите, какие меры безопасности, и ограничения доступа вы предпримете, чтобы гарантировать конфиденциальность и целостность данных в системе.

2. Какие основные цели применения информационных технологий в органах внутренних дел?

3. *Задание:* Составьте список основных целей применения информационных технологий в деятельности органов внутренних дел и объясните их значение.

4. Какое значение имеет использование баз данных и информационных систем для хранения и обработки информации о преступлениях, преступниках и жертвах?

5. *Задание:* Объясните, какие преимущества предоставляет использование баз данных и информационных систем для хранения и обработки информации о преступлениях, преступниках и жертвах.

6. Какие преимущества предоставляет электронное ведение учета и оперативный доступ к данным, включая паспортные и водительские удостоверения, информацию о судимости и другие важные документы?

7. *Задание:* Опишите основные преимущества электронного ведения учета и оперативного доступа к данным в сфере органов внутренних дел.

8. Какова роль создания и поддержки сетей связи в оперативном обмене информацией между отделениями и подразделениями органов внутренних дел?

9. *Задание:* Объясните важность создания и поддержки сетей связи для оперативного обмена информацией между отделениями и подразделениями

органов внутренних дел.

10. Какие основные принципы следует учитывать при создании и поддержке сетей связи в органах внутренних дел?

11. *Задание:* Составьте список основных принципов, которые необходимо учитывать при создании и поддержке сетей связи в органах внутренних дел, и объясните каждый из них.

Список литературы

1. Назмышев Р.А. Особенности и методические проблемы расследования неправомерного доступа к компьютерной информации. — Костанай, 2000. - С. 15.
2. Осипенко М. Компьютеры и преступность // Информационный бюллетень НЦБ Интерпола в Российской Федерации. - 1994. - № 10.
3. Андрианов В.И., Бородин В.А., Соколов А.В. «Шпионские штучки» и устройства защиты объектов информации: справочное пособие. - СПб., 1996.
4. Зубаха В.С., Усов А.И., Саенко Г.В., Волков ГА., Белый С.Л., Семикалепова А.И. Общие положения по назначению и производству компьютерно-технической экспертизы: методические рекомендации. - М., 2000.
5. Особенности производства обыска при расследовании компьютерных преступлений / М.М. Менжега. // Журнал российского права. - Декабрь 2003. - N 12. - С. 60.
6. Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений. – Москва, 2016.
7. Меллер К., Амуру А. Управление интернетом. – ОБСЕ, 2007.

ТЕМА 3. ПРИМЕРЫ ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ДЕЯТЕЛЬНОСТИ ОРГАНАХ ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ КАЗАХСТАНА

Цель: представить примеры применения информационных технологий в деятельности органов внутренних дел Республики Казахстана, чтобы понять и оценить важность и влияние информационных технологий на эффективность оперативных задач и обеспечение безопасности общества.

План:

1. Автоматизация оперативно-розыскной деятельности.
2. Создание и использование специализированных информационных систем для оперативного сбора, анализа и обработки данных.
3. Внедрение современных средств технического наблюдения, таких как видеонаблюдение, системы распознавания лиц и голоса, технологии анализа больших объемов данных.
4. Развитие электронных сервисов и систем.

1. Автоматизация оперативно-розыскной деятельности.

Роль специализированных информационных систем в органах внутренних дел:

Обеспечение оперативного сбора данных: Специализированные информационные системы позволяют собирать информацию о преступлениях, преступниках, жертвах и других событиях, связанных с правопорядком. Это включает в себя сбор данных о криминальных случаях, досье на подозреваемых и многие другие аспекты оперативной деятельности.

Анализ и обработка данных: Системы позволяют проводить анализ и обработку больших объемов данных для выявления закономерностей, связей и паттернов, помогая правоохранительным органам принимать взвешенные решения и предотвращать преступности.

Управление оперативной информацией: Специализированные системы обеспечивают эффективное хранение, организацию и доступ к оперативной информации, обеспечивая быстрый обмен данными между различными структурами правоохранительных органов.

Примеры применения специализированных информационных систем в Республике Казахстан:

- Единая информационная система «Кадры» (ЕИС «Кадры»): Эта система используется для учета и обработки информации о сотрудниках правоохранительных органов, включая персональные данные, служебную и карьерную информацию, обучение и др.
- Единая информационная система «Кризис» (ЕИС «Кризис»): Данная система предназначена для оперативного реагирования на кризисные ситуации,

обеспечивая сбор, анализ и обмен информацией между различными структурами правоохранительных органов в реальном времени.

2. Создание и использование специализированных информационных систем для оперативного сбора, анализа и обработки данных.

I. Значение специализированных информационных систем в органах внутренних дел РК

- Оперативный сбор информации: Специализированные информационные системы позволяют эффективно собирать информацию из различных источников, включая базы данных, открытые источники, свидетельства, документы и другие источники, что облегчает оперативное реагирование на преступления и другие происшествия.
- Анализ и обработка данных: Информационные системы обеспечивают средства для анализа и обработки больших объемов данных, позволяя выявлять связи, паттерны и тенденции, а также выявлять потенциально опасные ситуации и преступные группировки.
- Улучшение прогнозирования и планирования: Специализированные информационные системы предоставляют инструменты для прогнозирования и планирования оперативных мероприятий, помогая органам внутренних дел предотвращать преступления, оптимизировать ресурсы и улучшать безопасность общества.

Информационные технологии помогают органам внутренних дел более эффективно реагировать на преступления, предотвращать угрозы и обеспечивать безопасность общества. Использование специализированных информационных систем становится неотъемлемой частью деятельности органов внутренних дел и способствует более эффективной борьбе с преступностью в Республике Казахстан.

3. Внедрение современных средств технического наблюдения, таких как видеонаблюдение, системы распознавания лиц и голоса, технологии анализа больших объемов данных [1]

Эти инновационные технологии играют значительную роль в обеспечении безопасности, оперативного реагирования на происшествия и преступления, а также в расследовании преступлений.

1. Видеонаблюдение:

- Видеонаблюдение представляет собой систему, состоящую из камер, видеорегистраторов и других устройств, предназначенных для записи и передачи видеоинформации с целью обеспечения наблюдения за определенной территорией.
- Видеонаблюдение позволяет в режиме реального времени контролировать обстановку на объекте и записывать видеофрагменты для

последующего анализа и использования в расследовании преступлений.

2. Системы распознавания лиц и голоса:

- Системы распознавания лиц и голоса основаны на использовании алгоритмов и технологий, позволяющих идентифицировать и анализировать уникальные характеристики лица или голоса для их дальнейшего распознавания.
- Распознавание лиц и голоса применяется для идентификации подозреваемых, контроля доступа, поиска пропавших людей и многих других целей.

3. Технологии анализа больших объемов данных:

- Технологии анализа больших объемов данных (Big Data) предоставляют возможность обрабатывать и анализировать огромные объемы информации, собранные из различных источников, в том числе из видеонаблюдения, социальных сетей, электронной почты и других.
- Анализ больших данных позволяет выявлять паттерны, тренды, связи и аномалии, что помогает оперативным службам в прогнозировании и предотвращении преступлений, а также в эффективной расследовательной деятельности.

Примеры применения современных технических средств наблюдения [2]:

1. Видеонаблюдение на общественных местах: Установка камер видеонаблюдения на улицах, в парках, аэропортах, торговых центрах и других общественных местах позволяет следить за ситуацией, обеспечивать безопасность граждан и быстро реагировать на возможные происшествия.

2. Системы распознавания лиц и голоса в пунктах контроля: Применение систем распознавания лиц и голоса на пунктах контроля, таких как аэропорты, железнодорожные вокзалы и границы, позволяет автоматически идентифицировать подозреваемых, контролировать доступ и повышать безопасность пассажиров.

3. Анализ больших объемов данных в расследовательной деятельности: Использование технологий анализа больших данных позволяет обрабатывать информацию из различных источников, включая видеофрагменты, текстовые сообщения, телефонные разговоры и социальные сети, для выявления связей, образования преступных группировок и раскрытия преступлений.

Внедрение современных средств технического наблюдения, таких как видеонаблюдение, системы распознавания лиц и голоса, а также технологии анализа больших объемов данных, играет важную роль в оперативной деятельности органов внутренних дел Республики Казахстан. Эти инструменты помогают обеспечить безопасность, предотвращать преступления, эффективно расследовать и пресекать преступные активности. Их применение способствует улучшению качества работы правоохранительных органов и обеспечению безопасности граждан.

4. Развитие электронных сервисов и систем.

Внедрение электронных систем для подачи заявлений, получения разрешений и лицензий, что способствует снижению административной нагрузки и ускорению процедур [3].

1. Электронные системы для подачи заявлений:

- Электронные системы предоставляют гражданам и организациям возможность подать заявление или запрос на различные услуги через электронные платформы и порталы.
- Подача заявлений через электронные системы упрощает процесс, сокращает время и устраняет необходимость в физическом присутствии заявителя в офисе органов власти.

2. Электронные системы для получения разрешений и лицензий [4]:

- Электронные системы позволяют гражданам и организациям получать разрешения и лицензии через онлайн-платформы без необходимости личного посещения офисов и подачи бумажных документов.
- Внедрение электронных систем для получения разрешений и лицензий упрощает процесс, ускоряет его и позволяет сократить административную нагрузку на заявителей и государственные органы.

3. Снижение административной нагрузки:

- Снижение административной нагрузки означает упрощение процедур и процессов взаимодействия с государственными органами, устранение избыточной бюрократии и сокращение времени, затрачиваемого на оформление документов и получение разрешений.
- Внедрение электронных систем позволяет снизить административную нагрузку на заявителей, так как они могут подавать документы онлайн и получать результаты обработки своих заявлений в кратчайшие сроки.

4. Ускорение процедур:

- Ускорение процедур означает сокращение времени, необходимого для рассмотрения заявлений и выдачи разрешений и лицензий.
- Внедрение электронных систем позволяет автоматизировать процессы обработки документов, уменьшая человеческий фактор и ускоряя процедуры.

Примеры внедрения электронных систем в Республике Казахстан:

1. Единая портальная система «Электронное правительство»:

- В Казахстане внедрена единая портальная система "Электронное правительство", которая позволяет гражданам и организациям подавать заявления, получать разрешения и лицензии онлайн.
- Через эту систему можно получить различные государственные услуги, включая регистрацию бизнеса, получение строительных разрешений, оформление паспортов и водительских удостоверений и другие.

2. Электронная система подачи налоговой отчетности:

- Внедрение электронной системы подачи налоговой отчетности позволило гражданам и организациям в Республике Казахстан упростить процесс подачи налоговых деклараций и ускорить получение результатов.
- Через эту систему можно подавать налоговые отчеты, проверять статус

обработки документов и получать информацию о налоговых платежах.

3. Система электронного документооборота:

- Внедрение системы электронного документооборота позволяет государственным органам в Республике Казахстан эффективно обмениваться документами с гражданами и организациями.
- Через эту систему можно подавать заявления, получать разрешения и лицензии, обмениваться информацией и получать уведомления о статусе обработки документов.

Внедрение электронных систем для подачи заявлений, получения разрешений и лицензий в Республике Казахстан играет важную роль в снижении административной нагрузки на заявителей, ускорении процедур и повышении эффективности работы государственных органов. Эти системы обеспечивают удобство, доступность и безопасность взаимодействия между гражданами, организациями и государственными учреждениями.

Онлайн-мониторинг и предотвращение правонарушений в виртуальном пространстве, включая пресечение распространения незаконного контента и преступлений в сфере кибербезопасности.

В виртуальном пространстве происходят правонарушения, связанные с распространением незаконного контента и преступлениями в сфере кибербезопасности. В связи с этим в Республике Казахстан проводится онлайн-мониторинг и предпринимаются меры для предотвращения таких правонарушений.

1. Онлайн-мониторинг:

- Онлайн-мониторинг представляет собой систематическое наблюдение за активностью пользователей в интернете и анализ содержимого, размещенного ими.
- Цель онлайн-мониторинга состоит в обнаружении и предотвращении правонарушений, связанных с распространением незаконного контента и преступлениями в сфере кибербезопасности.

2. Распространение незаконного контента:

- Распространение незаконного контента включает размещение, обмен и распространение материалов, которые нарушают законодательство и могут включать в себя пиратское программное обеспечение, порнографию с участием несовершеннолетних, материалы, призывающие к насилию или терроризму и другие незаконные материалы.

3. Преступления в сфере кибербезопасности:

- Преступления в сфере кибербезопасности включают различные виды правонарушений, совершаемых в виртуальном пространстве, такие как хакерство, фишинг, вредоносные программы, кибершпионаж, кибертерроризм и другие.

Примеры применения онлайн-мониторинга и предотвращения правонарушений в виртуальном пространстве в Республике Казахстан:

1. Мониторинг социальных сетей и интернет-ресурсов:

- Правоохранительные органы проводят мониторинг социальных сетей и интернет-ресурсов для выявления и пресечения распространения незаконного

контента, включая порнографию с участием несовершеннолетних, экстремистские материалы и призывы к насилию.

- В случае обнаружения незаконного контента проводятся меры по его блокировке, удалению и привлечению виновных лиц к ответственности.

2. Системы фильтрации и блокировки:

- Создаются специализированные системы фильтрации и блокировки, которые позволяют автоматически определять и блокировать доступ к незаконному контенту и вредоносным ресурсам в сети Интернет.
- Эти системы позволяют быстро реагировать на новые угрозы и предотвращать их распространение.

3. Сотрудничество с интернет-провайдерами:

- С правоохранительными органами сотрудничают интернет-провайдеры, которые предоставляют информацию о пользователях, осуществляют блокировку доступа к незаконному контенту и содействуют в расследовании преступлений.

4. Развитие кадрового потенциала:

- Органы внутренних дел осуществляют обучение сотрудников по вопросам онлайн-мониторинга, предотвращения и расследования правонарушений в виртуальном пространстве.
- Проводятся тренировки и симуляции с целью повышения квалификации сотрудников и развития их навыков в области работы с современными средствами технического наблюдения и анализа данных.

Онлайн-мониторинг и предотвращение правонарушений в виртуальном пространстве являются важными аспектами обеспечения кибербезопасности и правопорядка в Республике Казахстан. С использованием современных технологий и специализированных систем органы внутренних дел успешно выявляют и пресекают распространение незаконного контента, а также предотвращают и расследуют преступления в сфере кибербезопасности. Это способствует поддержанию безопасной и законной среды в виртуальном пространстве и защите интересов граждан и общества в целом.

Вопросы и задания для самоконтроля:

1. *Задание №1:* Ваш отдел оперативного розыска получил задание собрать информацию о подозреваемом лице, которое требует большого объема оперативных данных из разных источников. Вы должны предложить решение для автоматизации сбора, анализа и обработки этих данных с помощью информационных технологий. Опишите, какие инструменты, и системы Вы используете для сбора и обработки оперативной информации и как они помогут улучшить эффективность вашей работы.

2. *Задание №2:* Вам поручено разработать специализированную информационную систему для Вашего отдела с целью оперативного сбора, анализа и обработки данных о преступлениях. Вы должны определить требования к системе, выбрать подходящие инструменты и разработать план внедрения. Предложите конкретные решения и обоснуйте их выбор с точки зрения эффективности и безопасности.

3. *Задание №3:* В вашем отделе возникла потребность в улучшении системы технического наблюдения и анализа данных для эффективного контроля и расследования преступлений. Вы ответственны за внедрение современных средств технического наблюдения, таких как видеонаблюдение, системы распознавания лиц и голоса, а также технологии анализа больших объемов данных. Опишите, какие конкретные технологии Вы планируете внедрить, и объясните, как они помогут улучшить оперативную деятельность и расследования в Вашем отделе.

4. *Задание №4*: Ваш отдел внутренних дел хочет разработать электронные сервисы и системы для улучшения взаимодействия с гражданами и оптимизации работы внутренних процессов. Вам поручено разработать план внедрения электронных сервисов, таких как онлайн-жалобы, электронный документооборот, электронное приемное окно и др. Опишите, какие конкретные сервисы Вы предлагаете разработать, и объясните, как они помогут улучшить качество обслуживания граждан и оптимизировать внутренние процессы в органах внутренних дел.

5. Какие преимущества может принести автоматизация оперативно-розыскной деятельности в органах внутренних дел?

6. Какие информационные технологии могут быть использованы для автоматизации оперативно-розыскной деятельности?

7. Какие задачи и функции оперативно-розыскной деятельности можно автоматизировать с помощью информационных технологий?

8. Какие вызовы и проблемы могут возникнуть при автоматизации оперативно-розыскной деятельности и как их можно преодолеть?

9. Какие основные преимущества предоставляют специализированные информационные системы для оперативного сбора, анализа и обработки данных?

10. Какие типы данных могут быть собраны, анализированы и обработаны с помощью специализированных информационных систем?

11. Какие методы и технологии используются для разработки специализированных информационных систем в органах внутренних дел?

12. Как эффективность оперативно-розыскной деятельности может быть улучшена с помощью специализированных информационных систем?

13. Какие возможности предоставляют современные средства технического наблюдения для оперативных служб в органах внутренних дел?

14. Какие технологии используются для видеонаблюдения, распознавания лиц и голоса, анализа больших объемов данных в контексте оперативно-розыскной деятельности?

15. Как современные средства технического наблюдения помогают в предотвращении и расследовании преступлений?

16. Какие этические и правовые вопросы связаны с использованием современных средств технического наблюдения в органах внутренних дел?

Список литературы

1. Комиссаров В., Гаврилов М., Иванов А. Обыск с извлечением

компьютерной и информации // Законность. - 1999. - № 3. – С. 90.

2. Шурухнов Н.Г., Лучин И.Н. Методические рекомендации по изъятию компьютерной информации при проведении обыска // Информационный бюллетень Следственного комитета МВД РФ. - М., 1996. - № 4(89).

3. Нугманова А.Т. (Завотпаева А.Т.) «Перспективные» проблемы организации проведения оперативно-розыскных мероприятий на сетях телекоммуникаций Республики Казахстан // Экономика и право Казахстана. — 2005. — № 11.

4. Лучин И.Н., Желдаков А.А., Кузнецов Н.А. Взламывание парольной защиты методом интеллектуального перебора // Информатизация правоохранительных систем. - М.: Академия МВД России, 1996.

ТЕМА 4. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И КИБЕРБЕЗОПАСНОСТИ: ЗАЩИТА ИНФОРМАЦИИ В ЦИФРОВОЙ ЭПОХЕ

Цель: ознакомить обучающихся с основными принципами и понятиями инофрмационной безопасности и кибербезопасности, а также предоставить им понимание важности защиты информации в современном цифровом мире.

План:

1. Введение в информационную безопасность.
2. Основные понятия кибербезопасности.
3. Кибербезопасность: актуальные угрозы и вызовы.
4. Роль сотрудников в обеспечении кибербезопасности: осведомленность и ответственность.
5. Разработка и внедрение систем мониторинга и обнаружения инцидентов информационной безопасности.

1. Введение в информационную безопасность.

Информационная безопасность – это состояние защищенности информации от угроз, рисков и несанкционированного доступа, а также обеспечение ее конфиденциальности, целостности и доступности. Она включает в себя комплекс мер и практик, направленных на защиту информационных ресурсов и систем от угроз, таких как кибератаки, вирусы, несанкционированный доступ, утечка информации и другие формы нарушения безопасности данных.

Информационная безопасность охватывает не только технические аспекты, но также требует внимания к организационным, процессным и человеческим аспектам. Она предполагает разработку и внедрение политик, процедур, технических решений и обучение персонала, чтобы обеспечить конфиденциальность, целостность и доступность информации.

Цель информационной безопасности заключается в обеспечении защиты конфиденциальности информации, предотвращении несанкционированного доступа и использования, защите данных от потери или повреждения, а также обеспечении надежности и непрерывности функционирования информационных систем и коммуникаций.

В современном информационном обществе, где цифровые технологии и интернет проникли во все сферы жизни, информационная безопасность стала критически важной. Она охватывает защиту конфиденциальности, целостности и доступности информации, а также обеспечивает защиту от киберугроз и киберпреступлений. Вот некоторые аспекты, подчеркивающие значение информационной безопасности в современном мире:

1. *Защита конфиденциальности:* Информация является ценным активом

для организаций и государств. Утечка конфиденциальных данных, таких как персональные данные клиентов, коммерческая информация или государственные секреты, может иметь серьезные последствия. Защита конфиденциальности является одним из основных аспектов информационной безопасности.

2. *Обеспечение целостности данных:* Целостность данных означает их неприкосновенность и защиту от несанкционированного изменения, подделки или повреждения. Поддержание целостности данных важно для предотвращения вмешательства и сохранения доверия к информации.

3. *Обеспечение доступности:* Информация должна быть доступна тем, кто имеет на то право и нуждается в ней для выполнения своих задач. Обеспечение доступности информации является ключевым аспектом информационной безопасности, чтобы предотвратить проблемы, связанные с недоступностью критической информации.

4. *Защита от киберугроз:* В современном мире информационные системы подвержены различным видам киберугроз, включая вирусы, вредоносные программы, фишинг, хакерские атаки и другие. Защита от этих угроз стала одной из основных задач информационной безопасности.

5. *Борьба с киберпреступностью:* Киберпреступления стали значительной проблемой в современном мире, и их воздействие на организации и государства может быть катастрофическим. Информационная безопасность играет важную роль в обнаружении, предотвращении и расследовании киберпреступлений.

6. *Защита критической инфраструктуры*: Критическая инфраструктура, такая как энергетические системы, телекоммуникации, финансовые институты и транспортные сети, является объектом повышенного внимания со стороны злоумышленников. Информационная безопасность играет важную роль в защите этой инфраструктуры от кибератак и обеспечении ее нормальной работы.

7. *Защита национальных интересов:* Информационная безопасность является неотъемлемой частью национальной безопасности. Государства разрабатывают стратегии и меры для защиты своей информационной инфраструктуры, государственных секретов и важных систем от внешних и внутренних угроз.

Основные составляющие национальных интересов:

1. Соблюдение конституционных прав и свобод человека и гражданина;
2. Информационное обеспечение государственной политики РК;
3. Развитие IT-технологий;
4. Защита информационных ресурсов от несанкционированного доступа.

Проблемные аспекты информационной безопасности:

✓ Несовершенство правовой базы;

✓ Негативное влияние на организацию информационной безопасности в стране;

✓ Отсутствие отечественных информационных технологий;

✓ Отсутствие сконцентрированной критической массы ученых в сфере

защиты информации;

✓ Информационное неравенство;

✓ Кибермошенничество.

Информационная безопасность имеет огромное значение в современном мире. Она обеспечивает защиту информации, конфиденциальности, целостности и доступности. Развитие информационной безопасности становится все более важным в условиях роста технологий и угроз. Государства, организации и каждый человек должны придавать этому вопросу должное значение и принимать соответствующие меры для обеспечения информационной безопасности.

2. Основные понятия кибербезопасности.

Кибербезопасность – это область, связанная с защитой компьютерных систем, сетей и данных от несанкционированного доступа, утечек информации, вредоносных атак и других киберугроз. Кибербезопасность имеет важное значение в современном информационном обществе, где множество организаций и частных лиц зависят от компьютерных систем и сетей для хранения, обработки и передачи конфиденциальной информации.

Усиление кибербезопасности представляет собой комплекс мер и действий, направленных на повышение уровня защиты компьютерных систем и данных от киберугроз. Это включает в себя применение технических, организационных и правовых мер для обнаружения, предотвращения, анализа и реагирования на кибератаки и другие киберугрозы.

Усиление кибербезопасности может включать следующие меры и действия:

1. Обновление программного обеспечения: Регулярное обновление операционных систем, приложений и антивирусных программ для исправления известных уязвимостей и получения новых функций безопасности.
2. Сильные пароли и многофакторная аутентификация: Использование сложных паролей и введение механизмов многофакторной аутентификации (например, пароль + SMS-код) для повышения защиты от несанкционированного доступа.
3. Обучение персонала: Проведение тренингов и обучающих программ для сотрудников, чтобы повысить их осведомленность о кибербезопасности и научить их узнавать и предотвращать потенциальные угрозы.
4. Защита сетей: Установка межсетевых экранов (firewalls), использование сетевых сегментов и сегментации сетей, мониторинг сетевого трафика и обнаружение вторжений для обеспечения безопасности сетевых ресурсов.
5. Шифрование данных: Применение криптографических методов шифрования для защиты конфиденциальности данных, передаваемых по сети или хранящихся на устройствах.
6. Регулярное резервное копирование данных: Создание резервных копий

важных данных и файлов для предотвращения потери информации при сбое системы или атаке.

7. Мониторинг и обнаружение угроз: Установка систем мониторинга и обнаружения вторжений для своевременного выявления аномалий и подозрительной активности в сети.

8. Разработка политик и процедур: Разработка и внедрение политик, процедур и стандартов безопасности, которые должны быть соблюдаемыми всеми сотрудниками и пользователями информационных систем.

Применение этих мер и действий помогает усилить кибербезопасность и снизить риск возникновения кибератак и утечки данных. Однако в силу постоянно развивающихся угроз и новых методов атак, важно оставаться внимательными и постоянно обновлять свои меры безопасности.

Шифрование – это процесс преобразования информации в такой формат, который делает ее непонятной или недоступной для неавторизованных лиц. Цель шифрования заключается в защите конфиденциальности данных и обеспечении их безопасности во время передачи или хранения.

В процессе шифрования исходные данные, которые называются открытым текстом, преобразуются с использованием определенного алгоритма и ключа шифрования. Результатом шифрования является зашифрованный текст, или шифротекст. Шифрование делает шифротекст непонятным для третьих лиц, которые не имеют доступа к ключу шифрования или не знают алгоритма шифрования.

Только получатель, зная правильный ключ шифрования и обратный алгоритм, может расшифровать шифротекст и восстановить исходные данные. Процесс расшифрования обратен процессу шифрования и использует ключ расшифрования.

Шифрование широко используется для обеспечения безопасности информации в различных сферах, включая коммуникации, хранение данных и транзакции. Оно применяется в системах электронной почты, банковских операциях, передаче данных через интернет, защите конфиденциальных документов и многом другом.

Примеры популярных алгоритмов шифрования включают Advanced Encryption Standard (AES), Data Encryption Standard (DES), RSA (Rivest-Shamir-Adleman), и множество других. Каждый алгоритм имеет свои особенности и уровень безопасности, и выбор конкретного алгоритма зависит от требований безопасности и сферы применения.

3. Кибербезопасность: актуальные угрозы и вызовы.

Целью данной темы является информирование и повышение осведомленности слушателей об актуальных трендах и проблемах в области кибербезопасности.

Угрозы и вызовы относятся к ситуациям или факторам, которые могут представлять потенциальные опасности, проблемы или вызовы для

безопасности, функционирования или развития чего-либо. В контексте кибербезопасности, угрозы и вызовы относятся к ситуациям, связанным с безопасностью информационных систем, данных и сетей.

Угрозы в кибербезопасности могут быть разнообразными и включать следующие аспекты:

1. Вредоносное программное обеспечение (Malware): это вредоносные программы, которые разработаны для причинения вреда системам, данных или пользователям. Это может включать вирусы, черви, троянские программы, шпионское программное обеспечение и другие.

2. Киберпреступники: это злоумышленники, которые осуществляют кибератаки с целью получения несанкционированного доступа к системам, кражи данных, мошенничества, шантажа и других преступлений в виртуальном пространстве.

3. Фишинг и социальная инженерия: это методы манипулирования людьми с целью получения конфиденциальной информации, такой как пароли, номера кредитных карт или другие личные данные. Например, фишинговые письма, подделка веб-сайтов или обман пользователей.

4. Денежные мошенничества и финансовые атаки: это кибератаки, направленные на финансовые системы, банки, платежные системы и другие финансовые институты с целью незаконного получения финансовой выгоды.

5. Утечка данных: это случаи, когда конфиденциальная информация становится доступной неавторизованным лицам. Утечка данных может привести к краже личных данных, коммерческой тайны, интеллектуальной собственности и другим негативным последствиям.

Вредоносное программное обеспечение (ВПО) представляет собой тип программного обеспечения, разработанного с целью нанесения вреда информационным системам, компьютерам и данным. Оно может иметь различные формы и функции, включая вирусы, черви и троянские программы.

Вот подробная информация о каждом из этих типов вредоносного ПО:

Вирусы: Вирус является программой, которая способна копировать себя и внедряться в другие программы или файлы. При запуске зараженного файла вирус может начать свое деструктивное действие, включая уничтожение данных, изменение функциональности системы или кражу конфиденциальной информации. Вирусы распространяются путем выполнения зараженных файлов или использования зараженных съемных носителей.

Черви: Червь представляет собой автономную программу, способную копировать себя и распространяться по сети без необходимости прикрепления к другим файлам. Черви могут использовать уязвимости в сетевых протоколах или операционных системах для автоматического распространения с одного компьютера на другие. Они могут наносить вред системам, потреблять ресурсы сети или выполнять другие злонамеренные действия.

Троянские программы: Троянские программы представляют собой программы, которые маскируются под полезные или легитимные приложения, но при этом выполняют скрытые и нежелательные действия. Они могут включать функции, такие как удаленный доступ к системе, кража

конфиденциальных данных, установка дополнительного вредоносного ПО или создание задней двери для дальнейшего вторжения злоумышленников.

Вредоносное ПО может быть распространено различными способами, включая прикрепление к электронным письмам, загрузку из небезопасных веб-сайтов, использование зараженных съемных носителей или эксплуатацию уязвимостей в программном обеспечении и операционных системах.

Заражение компьютера или информационной системы вредоносным ПО может иметь серьезные последствия. Оно может привести к потере данных, компрометации конфиденциальной информации, нарушению работы системы или даже угрожать безопасности организации или пользователей. Поэтому защита от вредоносного ПО и обеспечение безопасности информационных систем становятся критически важными в современном мире.

Вредоносное программное обеспечение (ВПО) может принимать различные формы и иметь разные цели.

Вот несколько примеров известных типов вредоносного ПО:

1. Вирус: Примером вируса является "ILOVEYOU", который был активен в 2000 году. Этот вирус распространялся через электронную почту и заражал компьютеры, заменяя файлы пользователя на свои копии и отправляя себя другим пользователям.

2. Червь: Известным примером червя является "WannaCry", который всплыл в 2017 году. Этот червь эксплуатировал уязвимость в операционной системе Windows и распространялся по сети, заражая компьютеры и шифруя файлы, требуя выкуп для их расшифровки.

3. Троянский конь: Примером троянского коня является "Zeus Trojan", который был разработан для кражи финансовых данных. Он маскировался под легитимные приложения и затем перехватывал логины, пароли и другую конфиденциальную информацию у пользователей.

4. Рансомваре: Один из известных примеров рансомвара - "Locky". Это вредоносное программное обеспечение шифровало файлы на компьютере пользователя и требовало выкуп для их разблокировки.

5. Шпионское ПО: Примером шпионского ПО является "Keylogger". Это программное обеспечение записывает все нажатия клавиш на компьютере пользователя, что позволяет злоумышленнику получить доступ к конфиденциальным данным, таким как пароли и банковские реквизиты.

Это только некоторые примеры вредоносного программного обеспечения, и существует множество других типов и вариантов. Важно понимать, что ВПО постоянно развивается, и поэтому необходимо принимать меры для обеспечения безопасности информационных систем и компьютеров.

Вызовы в кибербезопасности относятся к сложностям и проблемам, с которыми сталкиваются организации и отрасли в области обеспечения безопасности информационных систем и данных.

Это могут быть следующие аспекты:

1. *Постоянно развивающиеся угрозы:* киберугрозы постоянно эволюционируют, и новые методы и инструменты используются

злоумышленниками для обхода существующих мер безопасности.

2. *Недостатки в безопасности:* слабые места в системах и приложениях могут быть использованы злоумышленниками для совершения атак. Недостатки в безопасности могут быть связаны с программным обеспечением, конфигурацией сетей, ошибками в разработке или неправильной политикой безопасности.

1. **Авторизация** – это процесс предоставления разрешений и ограничений для доступа пользователя или устройства к определенным ресурсам или функциям системы.

2. **Шифрование** – это процесс преобразования информации в зашифрованный формат с использованием специальных алгоритмов, чтобы предотвратить несанкционированный доступ к данным.

3. **Межсетевой экран (firewall)** – это устройство или программное обеспечение, которое контролирует и фильтрует сетевой трафик, разрешая или блокируя соединения на основе заданных правил безопасности.

4. **Обновление (патч)** – это исправление программного обеспечения или операционной системы, которое выпускается разработчиками для устранения уязвимостей и ошибок, обнаруженных в предыдущих версиях.

Создание надежной цифровой защиты:

1. ***Оценка уязвимостей:*** Проведите анализ и оценку уязвимостей вашей информационной системы, чтобы определить слабые места и потенциальные угрозы.

2. ***Разработка политики безопасности:*** Создайте политику безопасности, которая определяет правила и меры для защиты информационных ресурсов организации. Включите в нее требования по паролям, доступу к данным, использованию защищенных соединений и другие аспекты безопасности.

3. ***Аутентификация и авторизация:*** Внедрите механизмы аутентификации и авторизации, такие как пароли, двухфакторная аутентификация и контроль доступа, чтобы гарантировать, что только правильные пользователи имеют доступ к системе и данным.

4. ***Шифрование данных:*** Примените шифрование для защиты конфиденциальности данных при их передаче и хранении. Используйте сильные шифровальные алгоритмы и ключи.

5. ***Установка межсетевого экрана (firewall):*** Установите и настройте межсетевой экран для контроля сетевого трафика, блокировки несанкционированных подключений и предотвращения вторжений.

6. ***Обновление программного обеспечения:*** Регулярно обновляйте операционные системы и программное обеспечение, чтобы закрыть известные уязвимости и получить последние исправления и патчи.

7. ***Обучение и осведомленность:*** Проводите обучение сотрудников по основам кибербезопасности, чтобы повысить их осведомленность о потенциальных угрозах и методах защиты. Сознательные пользователи могут быть первыми линиями защиты от атак.

8. ***Мониторинг и реагирование:*** Установите системы мониторинга и

инцидентного реагирования, чтобы обнаруживать и реагировать на потенциальные нарушения безопасности в реальном времени.

Примеры:

1. Установка брандмауэра для ограничения внешнего доступа к сети организации.
2. Внедрение системы антивирусной защиты для обнаружения и блокировки вредоносного программного обеспечения.
3. Обучение сотрудников правилам безопасного поведения в сети, таким как осведомленность о фишинговых атаках и запрет на открытие подозрительных вложений.
4. Использование системы мониторинга сетевой активности для обнаружения аномалий и потенциальных взломов.
5. Резервное копирование данных и создание системы восстановления для минимизации потерь при возможных инцидентах безопасности.

Внедрение надежной цифровой защиты в организации играет важную роль в предотвращении угроз и обеспечении безопасности информационных ресурсов. Организации должны уделять должное внимание кибербезопасности и применять соответствующие меры, чтобы защитить свои данные и системы от атак и несанкционированного доступа.

4. Роль сотрудников в обеспечении кибербезопасности: осведомленность и ответственность.

Конфиденциальность - это право на защиту личных данных, коммерческой информации, медицинских записей, банковских данных и другой чувствительной информации от несанкционированного доступа, использования или раскрытия [1].

Нарушение конфиденциальности означает неправомерное раскрытие или доступ к конфиденциальной информации или данных без согласия их владельца.

Нарушение конфиденциальности может происходить различными способами [2]:

1. *Несанкционированный доступ:* получение доступа к конфиденциальной информации без разрешения владельца, например, через хакерские атаки, взлом систем, подделку учетных записей или использование слабых паролей.
2. *Утечка информации:* раскрытие конфиденциальной информации неправомерным образом, каким-либо способом, например, через утрату или кражу физических носителей информации, несанкционированное раскрытие данных работниками или нарушение безопасности сетей и систем хранения данных.
3. *Нарушение связанной конфиденциальности:* нарушение договорных обязательств или соглашений о конфиденциальности, например, разглашение информации третьим лицам без согласия или нарушение условий договоров

или соглашений.

4. *Социальная инженерия:* использование манипуляции и обмана людей с целью получения доступа к конфиденциальной информации, например, через фишинговые атаки, обман или подмену личности.

Нарушение конфиденциальности может иметь серьезные последствия для физических лиц и организаций. Это может привести к утрате доверия, финансовым потерям, нарушению прав человека, утечке коммерческой тайны, краже личных данных и другим негативным последствиям. В связи с этим, защита конфиденциальности является важной составляющей информационной безопасности и требует применения соответствующих мер и технологий, таких как шифрование данных, управление доступом, аудит безопасности и обучение сотрудников по правилам конфиденциальности.

Потеря данных – это нежелательное событие, при котором информация, хранящаяся на компьютере, сервере, электронном устройстве или другом носителе данных, становится недоступной, повреждается, уничтожается или нечитаемой. Потеря данных может быть вызвана различными причинами, включая технические сбои, программные ошибки, вирусы и злонамеренные действия, физические повреждения носителя данных, а также человеческий фактор, такой как случайное удаление или неправильное использование данных [3].

Потеря данных может иметь серьезные последствия для организаций и отдельных лиц, включая финансовые потери, нарушение бизнес-процессов, утрату ценной информации, повреждение репутации и нарушение конфиденциальности. В некоторых случаях, особенно когда речь идет о чувствительных данных или персональной информации, потеря данных может также привести к нарушению законодательства и наказанию.

Для предотвращения потери данных и минимизации ее последствий важно принимать меры по обеспечению безопасности данных, такие как регулярное создание резервных копий, использование антивирусных программ и защищенных сетей, обучение сотрудников основам кибербезопасности, контроль доступа к данным и мониторинг системы на предмет необычной активности или потенциальных угроз.

Если потеря данных все же произошла, важно иметь план восстановления данных, который включает процедуры и инструменты для восстановления информации из резервных копий или других источников, а также для проведения анализа причин потери и предотвращения ее повторного возникновения.

Обеспечение надежности и безопасности данных, регулярные резервные копии и грамотное управление информацией являются важными компонентами эффективной стратегии по защите данных и предотвращению потерь.

Финансовые убытки представляют собой потерю денежных средств или финансовую негативную сторону в результате различных событий, рисков или неблагоприятных обстоятельств. Они могут возникать как в личной сфере, так и в деловой или организационной деятельности. Финансовые убытки могут

быть вызваны различными факторами, включая экономические потери, операционные неудачи, инвестиционные риски, катастрофические события, преступные действия, ошибки в управлении или другие негативные факторы [4].

Примеры финансовых убытков включают:

1. Убытки в результате неудачных инвестиций: потери на фондовом рынке, неправильное инвестирование средств, снижение стоимости активов.

2. Потери от кражи или мошенничества: финансовые потери, вызванные преступными действиями, включая кражу денежных средств или финансовую информацию.

3. Экономические убытки в результате стихийных бедствий: ущерб, вызванный природными катаклизмами, такими как наводнения, землетрясения, ураганы или пожары.

4. Потери от нарушения данных и кибератак: ущерб, связанный с хакерскими атаками, кражей конфиденциальной информации, нарушением безопасности сети или утечкой данных.

5. Финансовые убытки в результате судебных исков: потери, вызванные судебными разбирательствами, штрафами, компенсационными платежами или упущенными возможностями.

6. Потери в результате операционных ошибок: финансовые потери, связанные с ошибками в управлении, неэффективными процессами, неправильными решениями или плохой организацией работы.

Финансовые убытки могут иметь серьезные последствия для физических лиц, компаний и организаций, поэтому они требуют эффективного управления рисками и принятия мер по предотвращению и снижению потерь.

Роль сотрудников в обеспечении кибербезопасности заключается в их осведомленности о принципах и практиках безопасности информации, а также в их ответственности за соблюдение соответствующих политик и процедур.

Осведомленность и ответственность сотрудников играют ключевую роль в создании безопасной киберсреды в организации.

Осведомленность сотрудников означает их знание и понимание основных аспектов кибербезопасности. Это включает следующее:

1. Идентификация угроз: сотрудники должны быть осведомлены о различных видах киберугроз, таких как фишинг, вредоносные программы, социальная инженерия и другие, а также уметь распознавать и предотвращать такие атаки.

2. Правила и политики: сотрудники должны быть знакомы с политиками и правилами безопасности информации в организации, включая требования к паролям, использование устройств и программного обеспечения, обработку конфиденциальных данных и другие аспекты безопасности.

3. Уязвимости и защита: сотрудники должны понимать, какие уязвимости могут быть присутствующими в системах и сетях, а также знать о мероприятиях по защите их данных, таких как шифрование, антивирусные программы, бэкапы и другие.

Ответственность сотрудников *включает следующее:*

1. Соблюдение политик и процедур: сотрудники должны строго соблюдать политики и процедуры безопасности информации в организации, следовать инструкциям и рекомендациям по использованию систем и данных, а также сообщать о возможных нарушениях или угрозах.

2. Сохранение конфиденциальности: сотрудники должны быть ответственными за сохранение конфиденциальности информации и данных, с которыми они работают, и не разглашать их третьим лицам без разрешения.

3. Обучение и освещение: сотрудники должны активно участвовать в обучающих программах и мероприятиях, связанных с кибербезопасностью, а также информировать других сотрудников о возможных угрозах и о мерах по их предотвращению.

Роль сотрудников в обеспечении кибербезопасности необходима для создания культуры безопасности в организации. Осведомленность и ответственность каждого сотрудника помогают предотвращать инциденты безопасности, минимизировать риски и обеспечивать надежную защиту информации организации.

Злоумышленники (также известные как хакеры, киберпреступники или киберугрозы) - это лица или группы, которые занимаются незаконными действиями в киберпространстве с целью получения незаконной выгоды, нанесения ущерба или нарушения конфиденциальности, целостности или доступности информации [5].

Злоумышленники могут иметь различные мотивации и цели, включая финансовую выгоду, шпионаж, уничтожение данных, распространение вредоносных программ, мошенничество, нарушение конфиденциальности или причинение репутационного вреда. Они могут использовать различные методы и техники, включая взлом, фишинг, социальную инженерию, атаки с использованием вредоносных программ и другие.

Злоумышленники постоянно развивают свои навыки и используют новейшие технологии и инструменты для достижения своих целей. Их деятельность представляет серьезную угрозу для организаций, государственных учреждений, бизнесов и частных лиц, поскольку может привести к утечке конфиденциальной информации, финансовым потерям, нарушению репутации и другим негативным последствиям.

Для борьбы со злоумышленниками и защиты от киберугроз необходимо принимать меры по кибербезопасности, такие как использование сильных паролей, шифрования данных, обновление программного обеспечения, мониторинг сетевой активности, обучение сотрудников основам безопасности и внедрение защитных мероприятий, таких как брандмауэры, антивирусные программы и системы обнаружения вторжений.

Риск – это вероятность возникновения неблагоприятных событий или потерь, связанных с определенной деятельностью или принятием решений.

В контексте кибербезопасности, риск представляет собой возможность возникновения угрозы или нарушения безопасности информации, которое может привести к негативным последствиям.

Риски в кибербезопасности могут быть разнообразными и включать такие

аспекты, как утечка конфиденциальных данных, нарушение целостности информации, нарушение доступности систем и сервисов, финансовые потери, ущерб репутации и другие негативные последствия.

Определение и оценка рисков в кибербезопасности являются важными шагами для разработки эффективных стратегий защиты. Это включает идентификацию потенциальных угроз и уязвимостей, оценку вероятности и воздействия неблагоприятных событий, а также принятие мер для снижения рисков.

Управление рисками в кибербезопасности включает в себя разработку и реализацию политик, процедур и технических мер, направленных на предотвращение и смягчение угроз, а также на быстрое обнаружение и реагирование на инциденты. Это включает мониторинг сетевой активности, использование средств обнаружения и предотвращения инцидентов, резервное копирование данных, обучение сотрудников и другие меры по обеспечению безопасности информации.

Цель управления рисками в кибербезопасности – минимизировать потенциальные угрозы и потери, связанные с нарушением безопасности информации, и обеспечить надежную защиту информационных ресурсов организации или системы.

Хакеры – это люди, обладающие навыками и знаниями в области компьютерной техники и программирования, которые используют свои навыки для проникновения в компьютерные системы или сети, с целью получения несанкционированного доступа к информации, нанесения ущерба или кражи данных.

Хакеры могут разделяться на различные группы в зависимости от их мотивации и действий. Вот некоторые из них:

1. Этические хакеры (также известные как «белые шляпы») - это специалисты по кибербезопасности, которые используют свои навыки и знания для тестирования систем на уязвимости с разрешения и согласия владельцев систем. Их целью является обнаружение и устранение уязвимостей, а также повышение общего уровня безопасности.

2. Черные хакеры (или «крэкеры») - это злоумышленники, которые используют свои навыки для незаконного доступа к системам и сетям с целью получения конфиденциальной информации, совершения мошенничества или нанесения ущерба. Они обычно нарушают законодательство и преследуют личные выгоды или негативные цели.

3. Государственные хакеры - это хакеры, которые действуют от имени государства или государственных организаций. Они могут быть наняты для кибершпионажа, кибератак или других операций, связанных с национальной безопасностью и военными целями.

4. Хактивисты (или «киберактивисты») - это хакеры, которые используют свои навыки для поддержки определенных политических, социальных или идеологических целей. Они могут взламывать веб-сайты, организовывать киберпротесты или распространять информацию в целях активизма и пропаганды.

Важно отметить, что не все люди, связанные с компьютерной безопасностью, являются хакерами. Многие специалисты по кибербезопасности работают на защите систем и сетей, предотвращая атаки и обеспечивая безопасность информации.

5. Разработка и внедрение систем мониторинга и обнаружения инцидентов информационной безопасности.

Разработка и внедрение систем мониторинга и обнаружения инцидентов информационной безопасности играют важную роль в обеспечении безопасности информации в Республике Казахстан. Эти системы предназначены для отслеживания и обнаружения потенциальных угроз и аномальных событий в информационных системах организаций.

Вот некоторые важные аспекты разработки и внедрения систем мониторинга и обнаружения инцидентов информационной безопасности:

1. *Определение требований:* Прежде чем приступить к разработке системы мониторинга и обнаружения инцидентов, необходимо провести анализ рисков и определить требования организации. Это включает определение типов угроз и инцидентов, которые требуется обнаружить, а также установку необходимых метрик и параметров для мониторинга.
2. *Выбор подходящих инструментов:* Существует множество инструментов и технологий, которые могут быть использованы для реализации системы мониторинга и обнаружения инцидентов. Они могут включать в себя системы управления журналами событий (SIEM), интранет-контроль (IDS/IPS), анализаторы трафика и другие инструменты для обнаружения и анализа аномалий.
3. *Конфигурация и настройка:* Система мониторинга и обнаружения инцидентов должна быть правильно настроена для эффективного обнаружения угроз. Это включает настройку правил и сигнатур, настройку пороговых значений, определение идентификационной информации для отслеживания активности и другие параметры, которые помогут системе обнаруживать аномальное поведение.
4. *Интеграция с другими системами:* Система мониторинга и обнаружения инцидентов должна быть интегрирована с другими системами информационной безопасности организации, такими как системы предотвращения вторжений и системы управления уязвимостями. Это позволяет обеспечить более полную картину общей безопасности и своевременное реагирование на угрозы.
5. *Обучение и обновление:* Система мониторинга и обнаружения инцидентов требует постоянного обновления и обучения. Необходимо следить за новыми угрозами и атаками, а также обновлять и настраивать систему в соответствии с изменяющейся угрозовой ситуацией. Также важно обучать сотрудников организации использованию системы и реагированию на обнаруженные инциденты.

Примеры разработки и внедрения систем мониторинга и обнаружения инцидентов информационной безопасности в Республике Казахстан могут включать в себя создание центров оперативного реагирования на киберинциденты (CSIRT), развертывание систем SIEM для сбора и анализа журналов событий, использование интранет-контроля для обнаружения вторжений и других технических решений для обнаружения угроз. Эти примеры показывают, как системы мониторинга и обнаружения инцидентов могут быть применены для повышения уровня информационной безопасности в организациях Республики Казахстан.

Обучение сотрудников ОВД в области кибербезопасности, в том числе обнаружения и предотвращения киберпреступлений и хакерских атак.

Обучение сотрудников органов внутренних дел (ОВД) в области кибербезопасности является важным аспектом в борьбе с киберпреступлениями и хакерскими атаками в Республике Казахстан. Сотрудники ОВД играют ключевую роль в обнаружении, предотвращении и расследовании киберпреступлений, поэтому им необходимы соответствующие знания и навыки в области кибербезопасности.

Информация об обучении сотрудников ОВД в области кибербезопасности в Казахстане:

1. Осведомленность о киберпреступлениях: Сотрудники ОВД должны иметь хорошее понимание о различных типах киберпреступлений, таких как мошенничество, кража личных данных, распространение вредоносных программ и другие. Обучение должно включать изучение основных характеристик каждого типа киберпреступлений, их последствий и методов обнаружения.

2. Обнаружение и предотвращение киберпреступлений: Сотрудники ОВД должны обучаться методам обнаружения и предотвращения киберпреступлений. Это может включать развитие навыков анализа цифровых следов, использование специализированных инструментов и технологий для обнаружения аномалий и подозрительной активности, а также разработку проактивных стратегий и мер для предотвращения кибератак.

3. Технические навыки: Обучение сотрудников ОВД в области кибербезопасности должно включать основы технических навыков, таких как понимание работы компьютерных сетей, операционных систем, веб-технологий и криптографии. Это поможет им лучше понять технические аспекты киберпреступлений и эффективнее расследовать инциденты.

4. Сотрудничество и координация: Обучение должно также подчеркивать важность сотрудничества и координации с другими организациями и специалистами в области кибербезопасности. Сотрудники ОВД должны знать, как обмениваться информацией, работать вместе с цифровыми экспертами и специалистами по кибербезопасности, а также совместно расследовать и пресекать киберпреступления.

Примеры программ обучения сотрудников ОВД в Казахстане могут включать курсы и тренинги по следующим темам:

- Основы кибербезопасности и угрозы в сети
- Распознавание и обнаружение киберпреступлений
- Правовые аспекты кибербезопасности и киберпреступлений
- Методы и инструменты цифрового расследования
- Технические навыки и инструменты для обнаружения и анализа цифровых следов
- Сотрудничество с другими организациями и специалистами по кибербезопасности

Эти программы обучения помогут сотрудникам ОВД развить необходимые знания, навыки и осведомленность в области кибербезопасности, что в свою очередь способствует более эффективному обнаружению и предотвращению киберпреступлений в Республике Казахстан.

Вопросы и задания для самоконтроля:

1. *Задание №1:* Каковы основные компоненты треугольника кибербезопасности? Объясните каждый компонент и приведите примеры мер, которые могут быть приняты для обеспечения кибербезопасности в каждой из этих областей.
2. *Задание №2:* Какие наиболее распространенные угрозы в сфере кибербезопасности сталкиваются с организацией или органами внутренних дел? Опишите одну из этих угроз и объясните, как можно предотвратить или справиться с ней.
3. *Задание №3:* Сотрудник получил электронное письмо, содержащее подозрительную ссылку. Какие действия сотрудника могут способствовать обеспечению кибербезопасности? Назовите шаги, которые сотрудник должен предпринять, и почему каждый из них важен.
4. *Задание №4:* Организация решила внедрить систему мониторинга и обнаружения инцидентов информационной безопасности. Какие основные шаги необходимо предпринять при разработке и внедрении такой системы? Объясните каждый шаг и приведите примеры мер, которые могут быть приняты для обеспечения эффективной работы системы.
5. Что понимается под термином "кибербезопасность" и почему она важна?
6. Какие основные компоненты треугольника кибербезопасности?
7. Что такое уязвимость и как она связана с кибербезопасностью?
8. Какие меры могут быть приняты для обеспечения кибербезопасности?
9. Какие основные виды угроз существуют в сфере кибербезопасности?
10. Какие вызовы и сложности сталкиваются в области кибербезопасности сегодня?
11. Какие последствия могут возникнуть в результате кибератаки?
12. Какую роль играют сотрудники в обеспечении кибербезопасности организации?
13. Что означает осведомленность сотрудников в контексте кибербезопасности?
14. Какие меры можно предпринять для повышения осведомленности

сотрудников и их ответственности в области кибербезопасности?

15. Какие шаги необходимо выполнить при разработке системы мониторинга и обнаружения инцидентов информационной безопасности?

16. Какие инструменты и технологии могут быть использованы для создания такой системы?

17. Как система мониторинга и обнаружения инцидентов помогает в обеспечении кибербезопасности и своевременном реагировании на угрозы?

Список литературы

1. Алпеев А.С. Терминология безопасности: кибербезопасность, информационная безопасность. // Вопросы кибербезопасности. – 2014. -5 (8).

2. Федотов Н.Н. Форензика - компьютерная криминалистика. - Москва, 2007.

3. Безкоровайный М.М., Татузов А.Л. Кибербезопасность подходы к определению понятия. // Вопросы кибербезопасности. – 2014. - 1 (2).

4. Бураева Л.А. О некоторых вопросах обеспечения кибербезопасности в современных условиях. // Теория и практика общественного развития. - 2015. - 13.

5. Галатенко В.А. Основы информационной безопасности. Интернет-Университет Информационных Технологий (ИНТУИТ), 2008.

ТЕМА 5. ПЕРСПЕКТИВЫ РАЗВИТИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ КАЗАХСТАНА

Цель: представить и обсудить перспективы развития информационных технологий в органах внутренних дел Республики Казахстана с целью обеспечения более эффективной и современной работы в сфере правопорядка.

План:

1. Информационные системы в органах внутренних дел.
2. Основные понятия искусственного интеллекта.
3. Использование искусственного интеллекта (ИИ) и аналитики данных.
4. Применение ИИ и алгоритмов машинного обучения для автоматизации анализа данных, выявления паттернов и обнаружения преступлений.
5. Внедрение систем прогнозирования и моделирования для определения потенциальных угроз и разработки мер предупреждения преступлений.
6. Развитие системы электронного учета и контроля.
7. Интеграция информационных систем, таких как базы данных паспортов, водительских удостоверений и других документов, с целью повышения эффективности работы органов внутренних дел.
8. Внедрение электронных систем контроля и учета.

1. Информационные системы в органах внутренних дел.

Данные - это фиксированные сведения о событиях и явлениях, которые хранятся на определенных носителях [1].

Система — это сложный объект, состоящий из взаимосвязанных частей и существующий как единое целое [2].

Приказом МВД Республики Казахстан от 8 сентября 2014 года № 577 установлен порядок создания, использования и совершенствования ведомственных и оперативных учетов.

Объектами учета являются лица, факты (события), предметы (вещи), субъективные портреты, вещества и другие объекты, обладающие индивидуальной информацией, использование которой может способствовать профилактике, расследованию, раскрытию преступлений и розыску лиц, а также выполнению иных задач, возложенных на ОВД [3].

Информационная система – это система, предназначенная для хранения, обработки, поиска, распространения, передачи и предоставления информации с применением аппаратно-программного комплекса [4].

Ведомственный учет – это сбор, регистрация, обработка, накопление, систематизация, классификация и хранение сведений о лицах, предметах и событиях для обеспечения внутриведомственной деятельности ОВД [5].

«Система информационного обмена правоохранительных,

специальных государственных и иных органов» (СИО ПСО) - портал для получения необходимой информации правоохранительными и специальными органами из баз данных государственных органов в электронном виде, для оперативного реагирования и использования информации в служебных целях [6].

Целью системы информационного обмена является обеспечение оперативности, эффективности и координации работы между органами правоохранительной системы и другими специализированными органами государства. Она способствует сбору, обработке, передаче и хранению информации о преступлениях, преступниках, угрозах безопасности, розыске, профилактике и других сферах деятельности, связанных с обеспечением общественной безопасности.

Система информационного обмена включает в себя различные компоненты, такие как базы данных, сетевые инфраструктуры, программное обеспечение, протоколы связи и специализированные информационные системы. Она обеспечивает безопасность и конфиденциальность передаваемой информации, а также управление доступом к ней.

Система информационного обмена играет важную роль в повышении оперативности и эффективности работы правоохранительных органов и специализированных государственных органов. Она способствует сотрудничеству, совместным операциям, анализу и принятию обоснованных решений на основе актуальной и достоверной информации.

Дактилоскопическая система - это система и метод идентификации личности на основе уникальных папиллярных линий и паттернов на пальцах рук человека. Дактилоскопия является наукой, которая изучает уникальные особенности пальцевых отпечатков и их использование в идентификации и аутентификации личности [7].

Дактилоскопическая система работает на основе сбора, классификации, хранения и сравнения пальцевых отпечатков. Она использует специальные устройства, называемые дактилоскопами или сканерами отпечатков пальцев, для получения высококачественного изображения папиллярных линий на пальцах. Эти изображения затем анализируются и сравниваются с заранее сохраненными отпечатками в базе данных для определения совпадений или различий.

Дактилоскопия широко применяется в различных областях, включая правоохранительные органы, государственные учреждения, банковское дело, системы контроля доступа, миграционные службы, аэропорты и другие организации, где требуется точная идентификация личности.

Преимущества дактилоскопической системы включают [8]:

- Уникальность пальцевых отпечатков, каждый человек имеет уникальные паттерны, что делает их надежным биометрическим идентификатором.
- Устойчивость к изменениям, пальцевые отпечатки остаются практически неизменными в течение всей жизни человека.
- Высокая точность идентификации, дактилоскопическая система обладает высокой степенью точности при сопоставлении отпечатков пальцев.
- Быстрота и удобство использования, процесс сканирования и сравнения отпечатков пальцев может быть выполнен быстро и без необходимости использования сложного оборудования.

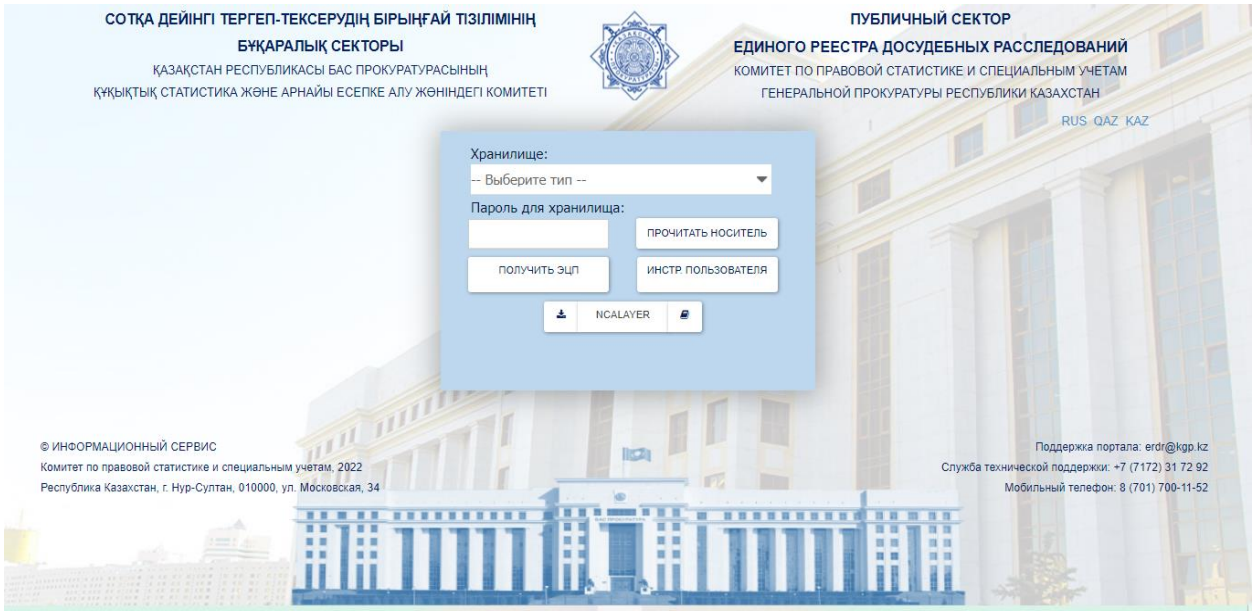
Дактилоскопическая информация – биометрические данные об особенностях строения папиллярных узоров пальцев и (или) ладоней рук человека или неопознанного трупа, позволяющие установить его личность, и персональные данные в соответствии с требованиями настоящего Закона (Закон Республики Казахстан от 30 декабря 2016 года № 40-VI ЗРК.)

Дактилоскопическая система является одним из наиболее распространенных и надежных методов биометрической идентификации, обеспечивая безопасность и защиту в различных сферах деятельности.

Министерство цифрового развития разработало программу создания национальной платформы **цифровой биометрической идентификации** на 2022–2024 годы.

Базовым элементом систем цифровой идентификации является сбор, хранение и обработка персональных биометрических данных — набора физических и поведенческих характеристик.

Информационная система «Единый реестр досудебных расследований» Комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан Подсистема «Публичный сектор».



Единый реестр досудебных расследований (ЕРДР) – это база данных, которая содержит информацию о проводимых досудебных расследованиях по уголовным делам. ЕРДР представляет собой систему, в которой собираются и хранятся сведения о фактах преступлений, лицах, участвующих в расследовании, принятых решениях и других релевантных данных.

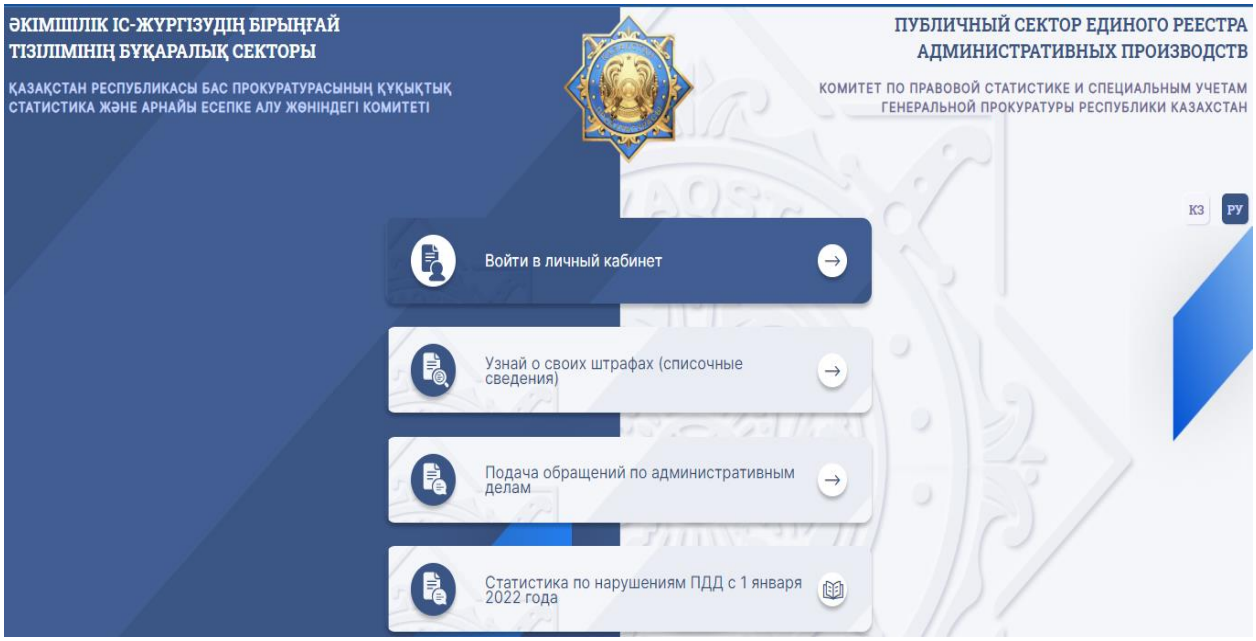
ЕРДР создан с целью обеспечения эффективности и прозрачности процесса досудебного расследования, а также для координации действий между различными участниками правоохранительной системы. Реестр позволяет упростить доступ к информации о ходе расследования, обеспечивает оперативный обмен данными между сотрудниками правоохранительных органов, судами, прокуратурой и другими участниками уголовного процесса.

В ЕРДР фиксируются следующие данные:

- Информация о преступлении, включая его характеристику, место и время совершения.
- Идентификационные данные подозреваемых, свидетелей и других участников дела.
- Сведения о проведенных оперативно-розыскных мероприятиях, допросах, экспертизах и других процессуальных действиях.
- Решения и постановления, вынесенные в рамках досудебного расследования.

ЕРДР является важным инструментом для организации правосудия и обеспечения прозрачности уголовного процесса. Он помогает сократить время и усилия при поиске информации о досудебном расследовании, а также обеспечивает возможность контроля и анализа данных для улучшения работы правоохранительных органов.

Единый реестр административных производств – информационная система, в которой содержаться вносимые сведения об административных правонарушениях, лицах, их совершивших, принятых по ним решениях, а также осуществляется ведение дел об административных правонарушениях в электронной форме.



Цель создания ЕРАП заключается в обеспечении эффективности и прозрачности процесса рассмотрения административных правонарушений, а также упрощении доступа к информации о нарушениях и принятых мерах ответственности. Реестр позволяет осуществлять оперативный обмен данными между различными участниками административного процесса, такими как правоохранительные органы, суды, органы местного самоуправления и другие организации, ответственные за рассмотрение административных дел.

В ЕРАП содержится следующая информация:

- Идентификационные данные нарушителя, включая его ФИО, дату рождения, паспортные данные и другую релевантную информацию.
- Описание административного правонарушения, включая характеристику нарушения, место и время его совершения.
- Решения и постановления, вынесенные в рамках административного производства, включая назначенные санкции и штрафы.
- Сведения о проведенных процессуальных действиях, таких как допросы, осмотры места нарушения и другие мероприятия.

ЕРАП имеет значение для организации и систематизации данных об административных правонарушениях, упрощения процедуры их рассмотрения и обеспечения доступа к информации для заинтересованных сторон. Реестр способствует повышению эффективности административного правосудия и обеспечению прозрачности процесса рассмотрения административных дел.

«Сергек» – это интеллектуальная система видеоконтроля, анализа и прогнозирования, включающая сеть модулей видеофиксации, контролирующих

ключевые зоны городского пространства – автотрассы, площади, транспортные развязки, придомовые территории.

Особенности модуля видеофиксации Сергек:

- Легкость монтажа
- Отсутствие проводных линий
- Высокая степень защиты от агрессивного воздействия окружающей среды
- Наличие программного комплекса распознавания автомобильных номеров

Модуль видеофиксации в режиме реального времени фиксирует и распознает номера попадающих в зону обзора автомобилей, а также параметров их движения и экологические показатели:

- Положение на дороге
- Скорость движения

Экологические датчики позволяют производить постоянный онлайн мониторинг состояния окружающей среды, в том числе:

- Концентрацию CO_2
- Уровень шума
- Атмосферное давление
- Влажность
- Температуру

Информация с видеокамер и датчиков по беспроводному каналу передается на серверы для последующей обработки.

Сергек располагает вычислительными мощностями и специальным программным обеспечением, позволяющими в режиме реального времени обрабатывать значительные объемы информации.

Функционал системы Сергек, в частности, включает:

- Фиксацию и прогнозирование автомобильного потока
- Выявление и отслеживание перемещения автомобилей с заданными параметрами движения, в том числе нарушителей правил дорожного движения (скорость, разметка)
- Оперативное информирование о важных событиях
- Сохранение и протоколирование объективной информации о важных событиях
- Трансляцию в режиме реального времени изображения с камер на мобильные устройства
- Сбор и анализ информации о параметрах автомобильных потоков и движении отдельных автомобилей

Функции системы «Сергек» адаптированны для правоохранительных органов. Исходя из функционала, система Сергек – это исключительно эффективное решение для широкого круга пользователей.

Интегрированный банк данных – это ведомственная информационная система центрального хранения и коллективного использования данных, содержащая информационные массивы, формируемые различными службами и подразделениями органов внутренних дел и других правоохранительных

органов, ведомств, взаимосвязанных между собой в едином банке данных. Целью формирования ИБД является эффективное информационное обеспечение органов внутренних дел, которое достигается путем постоянной актуализации данных, оперативного получения комплексной и систематизированной информации, в том числе посредством удаленного доступа.

Интегрированный банк данных имеет трех уровневую структуру формирования: формирование учетов районного уровня, формирование учетов областного уровня, формирование учетов республиканского уровня.

В интегрированном банке данных эксплуатируются следующие виды

1) формируемые в ИБД:

Криминальный автомототранспорт – информация о розыскиваемом и бесхозном автотранспорте. Настоящий учет предназначен для сбора, систематизации, хранения, обработки и выдачи в установленном порядке информациио розыскиваемых автомототранспортных средствах, транспортных средствах, принадлежность которых не установлена, а также представляющих оперативный интерес (сигнальный учет) имеющих номерную маркировку предприятия-изготовителя.

Учет используется при проведении оперативно-розыскных мероприятий, профилактике правонарушений, а также при регистрации перерегистрации транспортного средства в подразделениях административной полиции ОВД.

Криминальное оружие – информация о похищенном, утраченном, изъятом, добровольно сданном и добровольно возмездно сданном оружии. настоящий учет предназначен для сбора, систематизации, хранения, обработки и выдачи в установленном порядке информации о розыскиваемом, изъятом, добровольно сданном, добровольно возмездно сданном и обнаруженном оружии.

Криминальные вещи – информация о розыскиваемых вещах, имеющие идентификационный номер (в том числе сотовые телефоны). настоящий учет формируется в целях обеспечения розыска похищенных, утерянных и для установления принадлежности обнаруженных, добровольно сданных и изъятых на территории казахстана вещей, а также таврированного скота, похищенного на территории республики.

Криминальные документы – информация о похищенных, утраченных, изъятых и обнаруженных документах.

Розыск лиц – информация о розыскиваемых лицах. Настоящий централизованный учет предназначен для сбора, систематизации, хранения, обработки и выдачи в установленном порядке информации о розыскиваемых лицах, а также лицах, представляющих оперативный интерес.

Сигнальный учет – информация о лицах обоснованно-подозреваемых в совершеннии преступлений.

Подучетный элемент – информация о профиллактируемых лицах, а также лицах, представляющих оперативный интерес для органов внутренних дел. Настоящий учет предназначен для информационного обеспечения подразделений ОВД оперативно-статистическими сведениями о подучетных

лицах, с целью повышения эффективности деятельности по профилактике правонарушений, преступлений и предупреждению рецидивной преступности, а также оказания содействия при проведении оперативно-розыскных мероприятий и следственных действий. Постановке на учет подучетный элемент ИБД подлежит специальный контингент лиц. Основанием для постановки на учет являются материалы (приговор суда, справка об освобождении из мест лишения свободы, тебование о наличие судимости, обвинительный акт по уголовному делу, мотивированный рапорт инициатора постановки на учет).

Наркотики – Предприятия Трест – информация о юридических лицах, имеющих лицензию по осуществлению деятельности, связанную с оборотом наркотических средств, психотропных веществ и прекурсоров.

Зарегистрированное оружие – информация о зарегистрированном оружии и их владельцах, а также об оружии, находящемся на реализации в специализированных магазинах по торговле оружием на территории Республики Казахстан.

Интегрированный банк данных предполагает взаимосвязь и взаимодействие различных ведомств и органов. Благодаря единому банку данных информация становится доступной и используется несколькими ведомствами, что способствует координации и совместным действиям в области правоохранительной деятельности.

Таким образом, интегрированный банк данных играет важную роль в обеспечении централизованного хранения и коллективного использования информации между различными службами, подразделениями и ведомствами, что способствует более эффективной правоохранительной и оперативной деятельности.

Административная практика - это система сбора, регистрации и хранения информации о зарегистрированных административных правонарушениях. Она представляет собой базу данных, содержащую информацию о нарушениях административного законодательства, совершенных лицами или организациями.

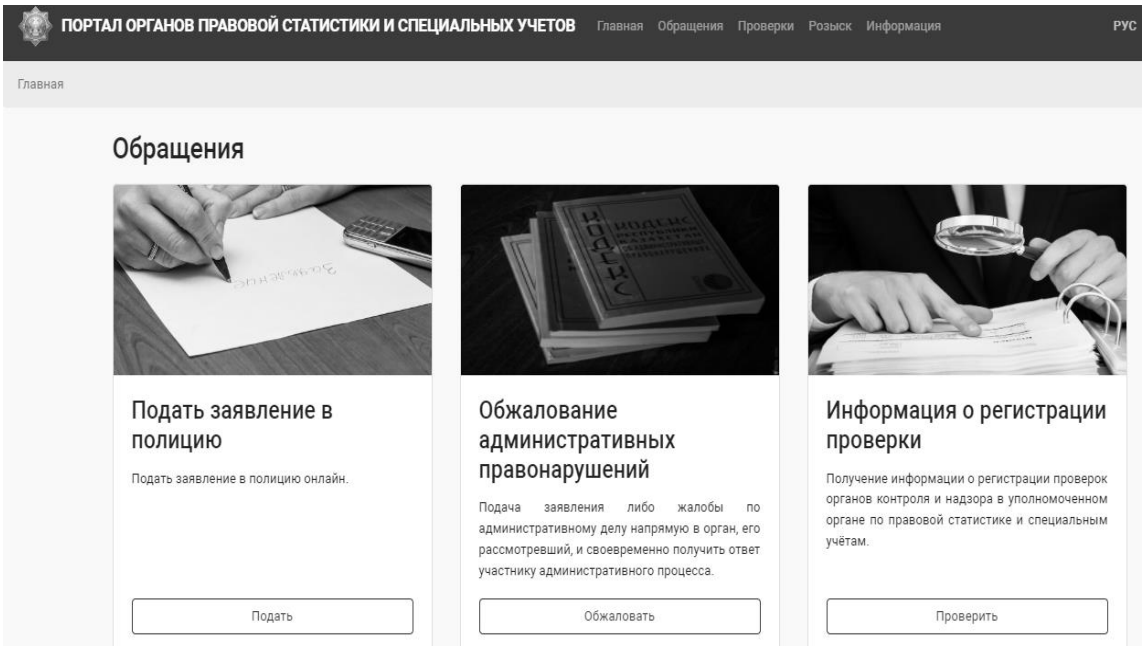
Административные правонарушения - это противоправные действия или бездействия, которые нарушают административное законодательство. Они могут включать различные нарушения в области дорожного движения, торговли, строительства, охраны окружающей среды, налогообложения и других сферах, регулируемых административными нормами.

Информация о зарегистрированных административных правонарушениях включает данные о нарушителях, описание правонарушений, дату и место их совершения, а также меры ответственности, принятые в отношении нарушителей.

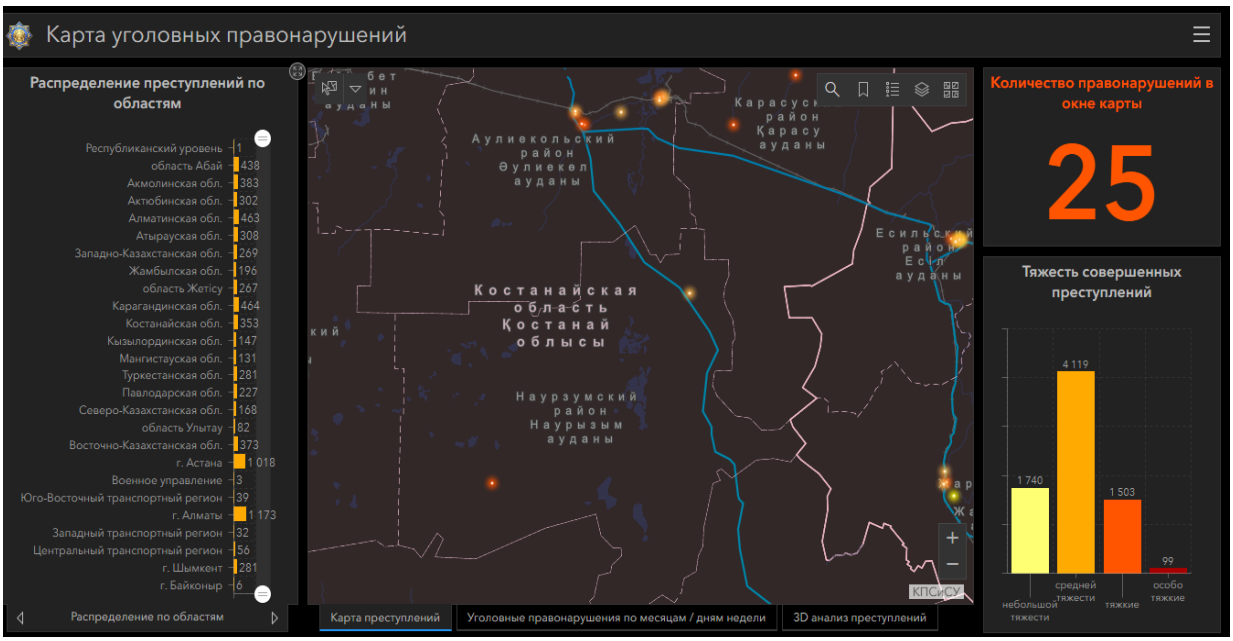
Административная практика играет важную роль в системе обеспечения исполнения административного законодательства. Она позволяет установить факты нарушений, вести статистику, контролировать соблюдение норм и принимать меры по предотвращению и пресечению административных правонарушений. Кроме того, информация об

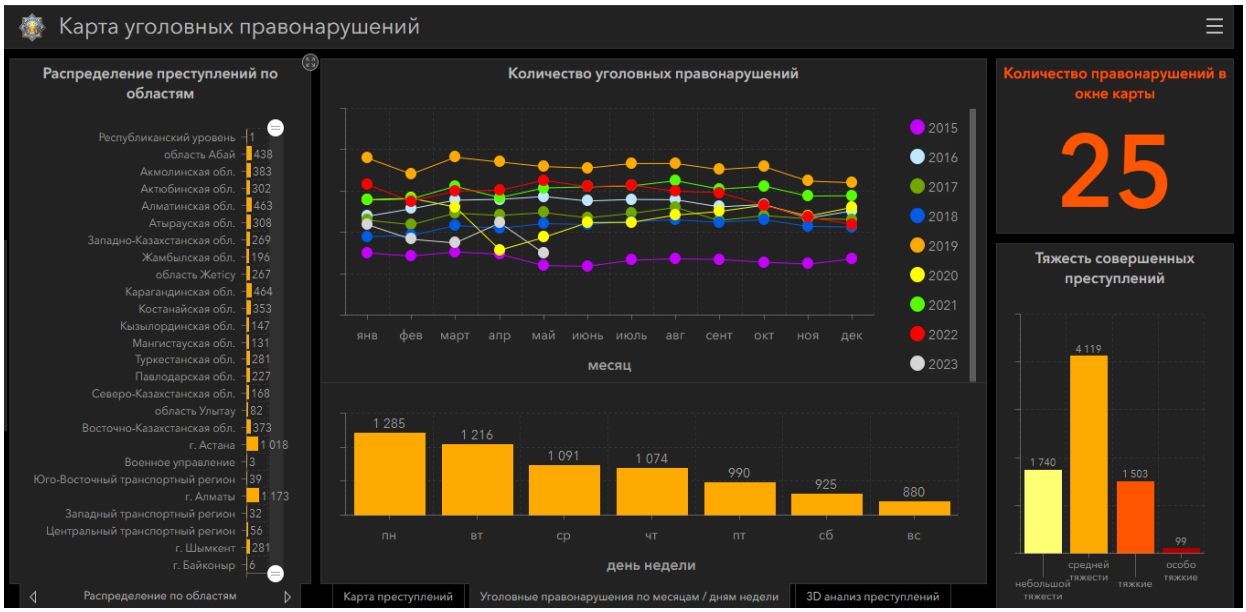
административных правонарушениях может использоваться в судебных процессах и в рамках административных расследований.

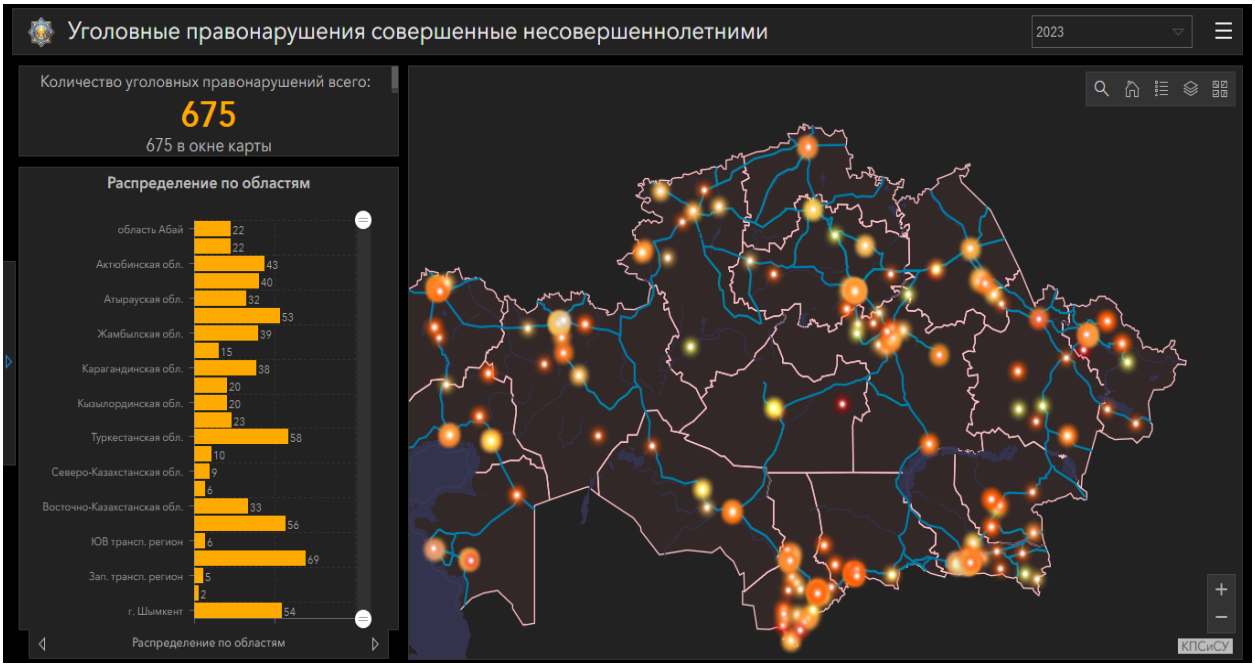
Портал органов правовой статистики и специальных учетов – Интернет-портал правовой статистики создан Комитетом по правовой статистике и специальным учётам Генеральной Прокуратуры Республики Казахстан в целях информирования граждан о состоянии преступности в стране и в отдельных её регионах, а также предоставлении интерактивных услуг.



Портал органов правовой статистики и специальных учетов содержит **«Географические карты»** для получения количественной информации в разрезе территориальности на карте страны по уголовным правонарушениям, в том числе совершенных несовершеннолетними; лиц, привлеченных к уголовной ответственности за совершение уголовных правонарушений против половой неприкосновенности несовершеннолетних; деятельности субъектов предпринимательства; зарегистрированных дорожно-транспортных происшествиях.


Карта уголовных правонарушений
Распределение преступлений по областям
Республиканский уровень 1
область Абай 438
Акмолинская обл. 383
Актюбинская обл. 302
Алматинская обл. 463
Атырауская обл. 308
Западно-Казахстанская обл. 269
Жамбылская обл. 196
область Жетісу 267
Карагандинская обл. 464
Костанайская обл. 353
Кызылординская обл. 147
Мангистауская обл. 131
Туркестанская обл. 281
Павлодарская обл. 227
Северо-Казахстанская обл. 168
область Улытау 82
Восточно-Казахстанская обл. 373
г. Астана 1 018
Военное управление 3
Юго-Восточный транспортный регион 39
г. Алматы 1 173
Западный транспортный регион 32
Центральный транспортный регион 56
г. Шымкент 281
г. Байконыр 6
Распределение по областям
Аулиекольский район Әулиекөл ауданы
Карасуский район Қарасу ауданы
Костанайская область Қостанай облысы
Наурзумский район Наурызым ауданы
КПСиСУ
Карта преступлений
Уголовные правонарушения по месяцам / дням недели
3D анализ преступлений
Количество правонарушений в окне карты
25
Тяжесть совершенных преступлений
1 740
4 119
1 503
99
небольшой тяжести
средней тяжести
тяжкие
особо тяжкие


Карта уголовных правонарушений
Распределение преступлений по областям
Республиканский уровень 1
область Абай 438
Акмолинская обл. 383
Актюбинская обл. 302
Алматинская обл. 463
Атырауская обл. 308
Западно-Казахстанская обл. 269
Жамбылская обл. 196
область Жетісу 267
Карагандинская обл. 464
Костанайская обл. 353
Кызылординская обл. 147
Мангистауская обл. 131
Туркестанская обл. 281
Павлодарская обл. 227
Северо-Казахстанская обл. 168
область Улытау 82
Восточно-Казахстанская обл. 373
г. Астана 1 018
Военное управление 3
Юго-Восточный транспортный регион 39
г. Алматы 1 173
Западный транспортный регион 32
Центральный транспортный регион 56
г. Шымкент 281
г. Байконыр 6
Распределение по областям
Количество уголовных правонарушений
янв фев март апр май июнь июль авг сент окт ноя дек
месяц
2015
2016
2017
2018
2019
2020
2021
2022
2023
1 285
1 216
1 091
1 074
990
925
880
пн вт ср чт пт сб вс
день недели
Карта преступлений
Уголовные правонарушения по месяцам / дням недели
3D анализ преступлений
Количество правонарушений в окне карты
25
Тяжесть совершенных преступлений
1 740
4 119
1 503
99
небольшой тяжести
средней тяжести
тяжкие
особо тяжкие



Портал органов правовой статистики и специальных учетов является важным инструментом для повышения прозрачности, эффективности и качества сбора и анализа данных в области правовой статистики. Он способствует улучшению мониторинга и изучения правонарушений, а также поддерживает разработку и реализацию эффективных стратегий в сфере правоохранительной деятельности.

2. Основные понятия искусственного интеллекта.

Искусственный интеллект (ИИ) – это область компьютерной науки, которая занимается разработкой и созданием компьютерных систем и программ, способных выполнять задачи, обычно требующие интеллектуальных способностей человека [9]. Искусственный интеллект стремится моделировать и эмулировать различные аспекты человеческого интеллекта, включая восприятие, обучение, решение проблем, анализ данных, планирование и принятие решений.

Основная идея искусственного интеллекта заключается в создании компьютерных систем, способных обрабатывать информацию и принимать решения на основе предоставленных им данных. Это достигается путем применения различных методов и техник, таких как машинное обучение, нейронные сети, символьные вычисления, генетические алгоритмы и другие.

Искусственный интеллект имеет широкий спектр применений во многих областях, включая медицину, финансы, транспорт, робототехнику, автоматизацию процессов и многие другие. Примеры применения искусственного интеллекта включают голосовых помощников, автоматическое распознавание речи, рекомендательные системы, анализ больших данных и автономные транспортные средства [10].

Одной из особенностей искусственного интеллекта является его способность к обучению на основе опыта и данных. Это означает, что системы и программы могут улучшать свою производительность и качество работы с течением времени, адаптируясь к новым ситуациям и обучаясь на основе накопленного опыта.

Однако, несмотря на все преимущества и достижения искусственного интеллекта, он также сопровождается рядом вызовов и этических вопросов, таких как приватность данных, безопасность, ответственность за принимаемые решения и вопросы, связанные с автономностью искусственных систем.

В целом, искусственный интеллект представляет собой мощный инструмент, который продолжает развиваться и находить новые применения в различных областях человеческой деятельности.

3. Использование искусственного интеллекта (ИИ) и аналитики данных.

Использование искусственного интеллекта (ИИ) и аналитики данных становится все более распространенным и значимым в различных сферах деятельности. Эти технологии предоставляют огромный потенциал для обработки, анализа и извлечения ценной информации из больших объемов данных, что позволяет принимать более обоснованные и эффективные решения [11].

Искусственный интеллект объединяет различные методы и подходы, которые позволяют компьютерным системам обучаться, адаптироваться и делать выводы из данных, аналогично способности человеческого интеллекта. Машинное обучение является одной из ключевых технологий искусственного интеллекта, которая позволяет системам самостоятельно извлекать закономерности и шаблоны из данных, чтобы делать прогнозы и принимать решения.

Аналитика данных включает в себя методы и инструменты для обработки и анализа данных с целью выявления скрытых паттернов, трендов и взаимосвязей. С помощью аналитики данных можно обрабатывать структурированные и неструктурированные данные, включая текстовые документы, изображения, видео, аудио и другие форматы. Это позволяет выявлять новые знания, прогнозировать события, оптимизировать процессы и принимать информированные решения.

Применение искусственного интеллекта и аналитики данных имеет широкий спектр применений в различных отраслях и областях, включая бизнес, медицину, финансы, производство, государственное управление и многое другое. Например:

1. В бизнесе и маркетинге: Искусственный интеллект и аналитика данных помогают анализировать поведение потребителей, прогнозировать спрос, оптимизировать ценообразование и рекламные кампании, а также улучшать процессы управления и принятия решений.

2. В медицине: Искусственный интеллект и аналитика данных применяются для диагностики болезней, прогнозирования рисков, разработки индивидуальных лечебных рекомендаций, анализа медицинских изображений и данных пациентов.

3. В финансовой сфере: Искусственный интеллект и аналитика данных используются для обнаружения мошенничества, анализа рынков, прогнозирования курсов валют, определения рисковых ситуаций и автоматизации процессов управления финансами.

4. В государственном управлении: Искусственный интеллект и аналитика данных применяются для анализа данных о населении, общественной безопасности, экономическом развитии, предоставлении государственных услуг и принятии решений на основе фактов и данных.

5. В производстве и технической сфере: Искусственный интеллект и аналитика данных применяются для управления производственными процессами, оптимизации энергопотребления, обнаружения неисправностей и предотвращения аварий, анализа больших объемов технических данных.

Внедрение искусственного интеллекта и аналитики данных требует квалифицированных специалистов, обладающих знаниями и навыками в области алгоритмов машинного обучения, статистики, анализа данных и программирования. Это также включает в себя этические аспекты, связанные с конфиденциальностью данных, прозрачностью алгоритмов и соблюдением законодательства в области защиты персональных данных.

В Республике Казахстан развитие и применение искусственного интеллекта и аналитики данных получает все большую поддержку и внимание. В рамках стратегии развития информационного общества в Казахстане принимаются меры по созданию специализированных центров, развитию инфраструктуры и обучению специалистов в области искусственного интеллекта и аналитики данных. Это способствует развитию инновационной экономики, повышению эффективности государственного управления и обеспечению безопасности информационных систем.

4. Применение ИИ и алгоритмов машинного обучения для автоматизации анализа данных, выявления паттернов и обнаружения преступлений.

Применение искусственного интеллекта (ИИ) и алгоритмов машинного обучения в области анализа данных и выявления преступлений становится все более значимым и эффективным [12]. Эти технологии позволяют автоматизировать процессы обработки больших объемов данных, выявлять скрытые паттерны и тренды, а также обнаруживать аномалии и потенциально преступные действия.

Применение ИИ и алгоритмов машинного обучения в анализе данных и выявлении преступлений может охватывать следующие аспекты:

Анализ больших данных: ИИ и алгоритмы машинного обучения

позволяют обрабатывать огромные объемы данных, включая структурированные и неструктурированные данные, такие как тексты, изображения, видео и аудио. Это позволяет выявлять скрытые паттерны и связи между данными, которые могут быть полезными при выявлении преступных действий [13].

Выявление аномалий: С помощью ИИ и алгоритмов машинного обучения можно разрабатывать модели, которые обучаются распознавать нормальные и аномальные паттерны в данных. Это позволяет выявлять аномалии и потенциально преступные действия, такие как финансовые мошенничества, кибератаки или незаконные действия.

Прогнозирование преступлений: Используя исторические данные о преступлениях и других факторах, ИИ и алгоритмы машинного обучения могут помочь в прогнозировании вероятности возникновения преступлений в определенных районах или ситуациях. Это позволяет правоохранительным органам принимать меры предотвращения и более эффективно распределять ресурсы.

Распознавание образов и лиц: Системы распознавания образов и лиц, основанные на ИИ и алгоритмах машинного обучения, используются для идентификации подозреваемых лиц на основе видеоматериалов или фотографий. Это помогает правоохранительным органам в выявлении преступников и предотвращении преступлений.

Анализ текстов: Алгоритмы обработки естественного языка и анализа текстов позволяют автоматически анализировать большие объемы текстовых данных, включая социальные сети, новостные статьи и сообщения. Это может помочь в выявлении угроз, дезинформации и других преступных действий.

В Республике Казахстан применение ИИ и алгоритмов машинного обучения в области анализа данных и выявления преступлений получает все большее внимание и поддержку. Это включает разработку специализированных систем мониторинга и обнаружения инцидентов информационной безопасности, обучение сотрудников правоохранительных органов в области кибербезопасности и киберпреступлений, а также сотрудничество с индустрией и академическими учреждениями для разработки и внедрения новых технологий в борьбе с преступностью.

5. Внедрение систем прогнозирования и моделирования для определения потенциальных угроз и разработки мер предупреждения преступлений.

Внедрение систем прогнозирования и моделирования является важным компонентом стратегии обеспечения кибербезопасности и борьбы с преступностью. Эти системы используются для анализа данных и создания моделей, которые помогают идентифицировать потенциальные угрозы и разрабатывать меры предупреждения преступлений.

Прогнозирование и моделирование в области безопасности основывается

на обработке больших объемов данных, включая информацию о предыдущих инцидентах, уязвимостях, трендах и других факторах, связанных с преступностью. На основе этих данных создаются модели, которые позволяют выявлять паттерны и прогнозировать вероятность возникновения определенных типов преступлений или угроз.

Применение систем прогнозирования и моделирования включает следующие аспекты:

Анализ данных: Системы прогнозирования и моделирования используют алгоритмы и методы анализа данных для обработки и структуризации информации о преступлениях, жертвах, подозреваемых, местоположениях и других факторах, влияющих на безопасность. Это позволяет выявлять связи и тренды, которые могут указывать на потенциальные угрозы.

Моделирование и симуляция: Системы прогнозирования и моделирования позволяют создавать модели и сценарии, которые отражают различные варианты развития событий и воздействия мер безопасности. Это помогает оценить эффективность различных мероприятий и прогнозировать их результаты.

Прогнозирование угроз: Используя данные и модели, системы прогнозирования могут определять потенциальные угрозы и риски на основе существующих данных и трендов. Это помогает организациям и правоохранительным органам принимать меры предупреждения и разрабатывать стратегии защиты.

Разработка мер предупреждения: Системы прогнозирования и моделирования помогают разрабатывать меры предупреждения преступлений и угроз. Это может включать определение оптимального размещения ресурсов безопасности, определение наиболее эффективных методов обнаружения и предотвращения преступлений, а также оптимизацию системы обеспечения безопасности.

Сотрудничество и обмен информацией: Внедрение систем прогнозирования и моделирования способствует сотрудничеству и обмену информацией между организациями, правоохранительными органами и другими заинтересованными сторонами. Обмен опытом и данными позволяет более точно прогнозировать и предупреждать угрозы, а также эффективнее реагировать на них.

В Республике Казахстан внедрение систем прогнозирования и моделирования для определения потенциальных угроз и разработки мер предупреждения преступлений имеет стратегическое значение. Оно позволяет организациям и правоохранительным органам эффективнее планировать и принимать меры для обеспечения безопасности, а также повышает оперативность и точность реагирования на угрозы и преступления.

6. Развитие системы электронного учета и контроля.

Развитие системы электронного учета и контроля играет важную роль в

эффективном управлении и контроле различных процессов в организациях и государственных структурах. Электронный учет и контроль предоставляют возможности для автоматизации, централизации и упрощения процессов учета, мониторинга и анализа данных.

Основные аспекты развития системы электронного учета и контроля включают:

Автоматизация учета: Электронная система учета позволяет автоматизировать процессы сбора, хранения и обработки данных о различных объектах и событиях. Например, это может быть система учета товаров на складе, финансовая система учета расходов и доходов организации или система учета рабочего времени сотрудников. Автоматизация учета устраняет ручной трудозатратный процесс и снижает вероятность ошибок.

Централизация данных: Электронная система учета и контроля позволяет централизованно хранить и управлять данными. Это обеспечивает доступность и единообразие данных для всех заинтересованных сторон. Например, система электронного учета может обеспечивать доступ к информации о клиентах, заказах, платежах и других ключевых аспектах бизнеса.

Мониторинг и контроль: Электронная система учета и контроля позволяет осуществлять непрерывный мониторинг и контроль за различными процессами и операциями. Например, это может быть система мониторинга безопасности, которая оповещает о нарушениях и необычных событиях в реальном времени. Также система может предоставлять аналитические инструменты для выявления трендов и аномалий, что помогает в принятии оперативных решений.

Анализ данных: Развитие системы электронного учета и контроля включает разработку аналитических инструментов и методов для анализа данных. Это позволяет проводить комплексный анализ данных, выявлять паттерны, тенденции и связи, а также прогнозировать возможные сценарии развития событий. Аналитика данных помогает в принятии стратегических решений и оптимизации процессов в организации.

Развитие системы электронного учета и контроля в Республике Казахстан способствует повышению прозрачности, эффективности и безопасности бизнес-процессов, а также обеспечивает более точное и оперативное принятие управленческих решений. Организации и государственные структуры активно внедряют системы электронного учета и контроля, чтобы улучшить свою работу и обеспечить эффективное управление ресурсами и процессами.

7. Интеграция информационных систем, таких как базы данных паспортов, водительских удостоверений и других документов, с целью повышения эффективности работы органов внутренних дел.

Интеграция информационных систем, таких как базы данных паспортов, водительских удостоверений и других документов, играет важную роль в

повышении эффективности работы органов внутренних дел в Республике Казахстан. Это позволяет упростить и ускорить процессы проверки и обработки информации, а также повысить точность и достоверность данных.

Основные аспекты интеграции информационных систем в органах внутренних дел включают:

1. Централизованное хранение данных: Интеграция различных информационных систем позволяет централизованно хранить данные о гражданах, их документах и других релевантных информациях. Это обеспечивает доступность и единообразие данных для всех подразделений и сотрудников органов внутренних дел.

2. Оптимизация процессов проверки и обработки данных: Интеграция информационных систем позволяет автоматизировать процессы проверки и обработки данных. Например, при проверке личных данных гражданина или водительского удостоверения, система может автоматически обращаться к соответствующим базам данных и получать необходимую информацию. Это ускоряет процессы работы и снижает вероятность ошибок.

3. Повышение качества данных: Интеграция информационных систем позволяет обновлять и синхронизировать данные в режиме реального времени. Например, при изменении информации в одной системе (например, при замене паспорта), эта информация автоматически обновляется в других связанных системах. Это позволяет поддерживать актуальность и достоверность данных.

4. Улучшение аналитики и расследований: Интеграция информационных систем позволяет проводить более глубокий анализ данных и расследований. Связывая различные типы данных и информацию, система может выявлять паттерны, связи и аномалии, что помогает в выявлении и предотвращении преступлений.

Интеграция информационных систем в органах внутренних дел Республики Казахстан способствует повышению оперативности, эффективности и качества работы, а также улучшает взаимодействие и координацию между различными подразделениями. Это позволяет более эффективно бороться с преступностью, обеспечивать безопасность и защиту прав граждан.

8. Внедрение электронных систем контроля и учета.

Внедрение электронных систем контроля и учета, таких как системы распознавания номерных знаков автомобилей и системы автоматического распознавания лиц, имеет важное значение для обеспечения безопасности и повышения эффективности работы органов внутренних дел в Республике Казахстан. Эти системы основаны на применении передовых технологий и алгоритмов, позволяющих автоматически и точно идентифицировать и регистрировать информацию о транспортных средствах и лицах.

Система распознавания номерных знаков автомобилей (Automatic Number Plate Recognition, ANPR) использует камеры и специальное программное

обеспечение для автоматического считывания и распознавания номерных знаков автомобилей. Эта система позволяет оперативно получать информацию о транспортных средствах, проверять их наличие в базах данных, контролировать скоростной режим, распознавать угнанные или участвующие в преступлениях автомобили и т.д. Это сокращает время и усилия, затрачиваемые на ручной ввод данных и проверку номерных знаков, и повышает эффективность работы правоохранительных органов.

Система автоматического распознавания лиц (Facial Recognition System) использует алгоритмы и методы компьютерного зрения для идентификации и регистрации лиц. Она может быть интегрирована в видеонаблюдение или другие системы безопасности для автоматического обнаружения и распознавания лиц на основе предварительно созданных баз данных. Это позволяет оперативно идентифицировать потенциально опасные личности, контролировать доступ в ограниченные зоны, расследовать преступления и обеспечивать безопасность общественных мероприятий.

Внедрение электронных систем контроля и учета в Республике Казахстан имеет ряд преимуществ:

Автоматизация процессов: Электронные системы позволяют автоматизировать процессы контроля и учета, снижая необходимость в ручном вводе данных и уменьшая вероятность ошибок. Это сокращает время, затрачиваемое на проверку и обработку информации.

Увеличение точности и надежности: Технологии распознавания номерных знаков автомобилей и лиц обладают высокой точностью и надежностью в идентификации объектов. Это позволяет более эффективно выявлять и регистрировать информацию о транспортных средствах и лицах, связанных с преступной деятельностью.

Усиление безопасности: Электронные системы контроля и учета помогают усилить безопасность, обнаруживая потенциально опасные ситуации, идентифицируя преступников и предотвращая преступления. Это способствует созданию безопасной и защищенной среды для граждан.

Улучшение оперативности и эффективности: Благодаря автоматическому считыванию и обработке данных, электронные системы контроля и учета позволяют оперативно реагировать на события, сокращают время обработки информации и улучшают общую эффективность работы органов внутренних дел.

Внедрение электронных систем контроля и учета, таких как системы распознавания номерных знаков автомобилей и системы автоматического распознавания лиц, является важным шагом в развитии органов внутренних дел Республики Казахстан. Они обеспечивают более эффективное и точное контролирование транспортных средств и лиц, способствуют превентивным мерам безопасности и обеспечивают более оперативное реагирование на преступные действия.

Вопросы для самоконтроля:

1. Какие основные характеристики определяют искусственный интеллект?
2. Приведите примеры приложений искусственного интеллекта в повседневной жизни.
3. Какие основные методы используются в искусственном интеллекте?
4. Как ИИ и аналитика данных помогают в принятии решений и оптимизации бизнес-процессов?
5. Приведите примеры использования ИИ и аналитики данных в различных отраслях.
6. Какие методы анализа данных широко применяются с использованием ИИ?
7. Какие методы машинного обучения применяются для обнаружения преступлений?
8. Какие данные могут быть использованы для обучения моделей машинного обучения в контексте преступности?
9. Какие проблемы могут возникнуть при применении ИИ и машинного обучения в области правоохранительной деятельности?
10. Какие методы прогнозирования и моделирования могут быть использованы для определения потенциальных угроз и преступлений?
11. Какие данные и параметры могут быть включены в модели для прогнозирования преступлений?
12. Какие действия и меры предосторожности могут быть предприняты на основе результатов прогнозирования?
13. Какие преимущества предоставляет система электронного учета и контроля по сравнению с традиционными методами?
14. Какие данные могут быть включены в систему электронного учета и контроля?
15. Какие вызовы могут возникнуть при внедрении и использовании системы электронного учета и контроля?
16. Какие типы электронных систем контроля и учета могут быть использованы в органах внутренних дел?
17. Какие выгоды может предоставить внедрение электронных систем контроля и учета?
18. Как обеспечить безопасность и защиту данных в электронных системах контроля и учета?

Список литературы

1. О ратификации Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в области обеспечения информатизационной безопасности: Закон Республики Казахстан от 3 мая 2018 года.
2. О Концепции информационной безопасности Республики Казахстан до 2016 года: Указ Президента Республики Казахстан от 14 ноября 2011 года № 174.

3. Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности: Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 (с изменениями и дополнениями от 10.02.2023 г.).

4. Об утверждении Концепции кибербезопасности «Киберщит Казахстана»: Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 (с изменениями и дополнениями от 17.03.2023 г.)

5. Алпеев А.С. Терминология безопасности: кибербезопасность, информационная безопасность. // Вопросы кибербезопасности. – 2014. - 5 (8).

6. Федотов Н.Н. Форензика - компьютерная криминалистика. - Москва, 2007г.

7. Безкоровайный М.М., Татузов А.Л. Кибербезопасность подходы к определению понятия. // Вопросы кибербезопасности. – 2014. - 1 (2).

8. Бураева Л.А. О некоторых вопросах обеспечения кибербезопасности в современных условиях. // Теория и практика общественного развития. – 2015. 13.

9. Галатенко В.А. Основы информационной безопасности. Интернет-Университет Информационных Технологий (ИНТУИТ), 2008.

10. Карасев П.А. Политика безопасности США в глобальном информационном пространстве. – Москва, 2015.

11. Старовойтов А.В. Кибербезопасность как актуальная проблема современности. // Информатизация и связь. – 2011. – 6. – С. 4-7.

12. Сырбу А.В. Процессуальный порядок получения и использования информации с технических каналов связи в уголовном судопроизводстве: дис. канд. юрид. наук. — Караганда, 2005.

13. Анин Б.Ю. Защита компьютерной информации. — СПб.: БХВ-Петербург, 2000. - 384 с.

ПРАКТИЧЕСКАЯ РАБОТА №1

Тема: Основополагающие документы в области информационной безопасности Республики Казахстан.

Цель работы: изучить основополагающие документы в области информационной безопасности и казахстанские и международные, которые используются в Казахстане.

Задание:

Изучить нормативно-правовые базы и составить краткий отчет по теме практической работы согласно следующей структуре:

1. Титульный лист
2. Содержание
3. Практическое задание
4. Конспект документа
5. Выводы

Список литературы

1. О ратификации Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в области обеспечения информатизационной безопасности: Закон Республики Казахстан от 3 мая 2018 года.
2. О Концепции информационной безопасности Республики Казахстан до 2016 года: Указ Президента Республики Казахстан от 14 ноября 2011 года № 174.
3. Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности: Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 (с изменениями и дополнениями от 10.02.2023 г.).
4. Об утверждении Концепции кибербезопасности «Киберщит Казахстана»: Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 (с изменениями и дополнениями от 17.03.2023 г.).
5. Алпеев А.С. Терминология безопасности: кибербезопасность, информационная безопасность. // Вопросы кибербезопасности. – 2014. - 5 (8).
6. Федотов Н.Н. Форензика - компьютерная криминалистика. - Москва, 2007.
7. Безкоровайный М.М., Татузов А.Л. Кибербезопасность подходы к определению понятия. // Вопросы кибербезопасности. – 2014. 1 (2).
8. Бураева Л.А. О некоторых вопросах обеспечения кибербезопасности в современных условиях. // Теория и практика общественного развития. – 2015. 13.
9. Галатенко В.А. Основы информационной безопасности. Интернет-Университет Информационных Технологий (ИНТУИТ), 2008.

10. Карасев П.А. Политика безопасности США в глобальном информационном пространстве. – Москва, 2015.
11. Старовойтов А.В. Кибербезопасность как актуальная проблема современности. // Информатизация и связь. - 2011. – 6. – С. 4-7.

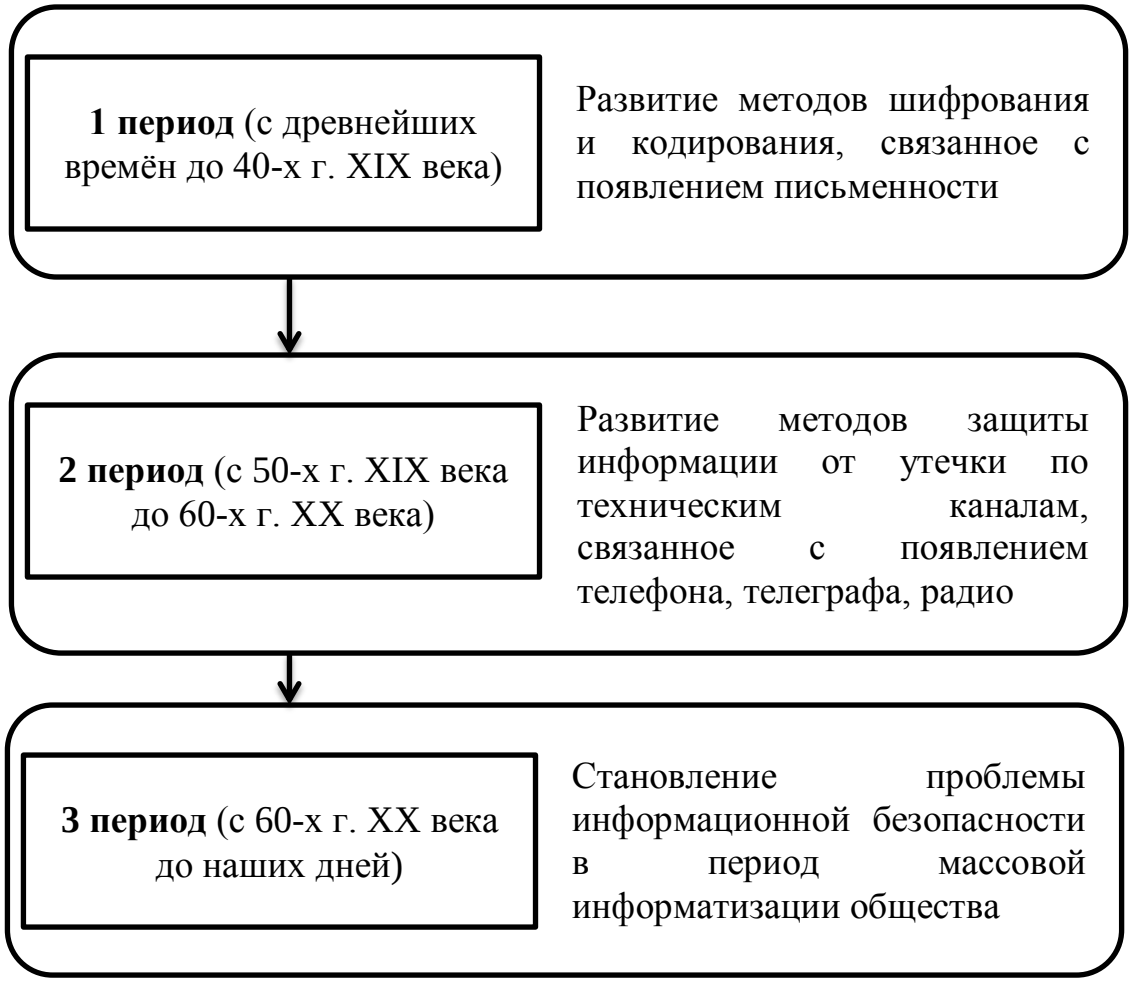
ПРАКТИЧЕСКАЯ РАБОТА №2

Тема: Обеспечение информационной безопасности в ведущих зарубежных странах

Цель работы: ознакомление с основными принципами обеспечения информационной безопасности в ведущих зарубежных странах.

Теоретическая часть

Защита информации всегда была важной проблемой для человечества. В ходе развития цивилизации менялись виды информации, а также применяемые для её защиты методы и средства. Процесс развития средств и методов защиты информации можно разделить на три относительно самостоятельных периода:



В последние годы мы наблюдаем значительное развитие информационных технологий, что может привести к возникновению новых форм борьбы, в том числе на межгосударственном уровне. Информационная война становится все более значимым элементом внешней политики, применяемым для защиты государственных интересов и достижения своих целей через различные формы воздействия. В связи с этим, важно изучить

основные принципы обеспечения информационной безопасности в ведущих зарубежных странах.

Еще одной причиной, почему полезно ознакомиться с политикой информационной безопасности зарубежных стран, является то, что большинство используемых в нашей стране средств и методов обеспечения информационной безопасности основаны на импортных методиках и компонентах. Эти методики и компоненты разработаны в соответствии с нормами и требованиями обеспечения информационной безопасности в странах-производителях. Поэтому перед изучением конкретных технологий и средств обеспечения информационной безопасности, необходимо понять политику информационной безопасности ведущих зарубежных стран.

Изучение политики информационной безопасности зарубежных стран поможет нам получить ценные знания и опыт, которые могут быть применены при разработке и реализации мер по обеспечению информационной безопасности в нашей стране. Это позволит нам лучше понять современные требования и подходы к обеспечению безопасности информации, а также сделать осознанный выбор в отношении используемых методик и компонентов.

В целом, изучение политики информационной безопасности зарубежных стран является важным шагом для обеспечения надежной защиты информации и адаптации к современным вызовам и угрозам в сфере информационной безопасности.

Задание:

1. Подготовить краткий доклад по заданному вопросу, используя учебное пособие Аверченкова В.И. «Системы защиты информации в ведущих зарубежных странах» и другие доступные источники информации.

Оформить доклад согласно следующей структуре:

1. Титульный лист
2. Содержание
3. Практическое задание
4. Конспект документа
5. Выводы

2. Заполнить таблицу «Системы обеспечения ИБ в Республики Казахстан и ведущих зарубежных странах» (см. таблица 1) на основе подготовленного материала, а также докладов других обучающихся.

Таблица 1. Системы обеспечения ИБ в Республики Казахстан и ведущих зарубежных странах.

№	Страна	Основные принципы обеспечения информационной безопасности	Основные документы в области обеспечения информационной безопасности	Структура государственнх органов обеспечения национальной информационной безопасности
1	Казахстан			
2	Италия			
3	США			
4	Великобритания			
5	Швеция			
6	Франция			
7	Германия			
8	Китай			
9	Япония			
10	Швейцария			
11	Испания			
12	Канада			
13	Австралия			
14	Бразилия			
15	Аргентина			
16	Корея			

Список литературы

1. О ратификации Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в области обеспечения информатизационной безопасности: Закон Республики Казахстан от 3 мая 2018 года.

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

3. Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности: Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 (с изменениями и дополнениями от 10.02.2023г.).

4. Об утверждении Концепции кибербезопасности «Киберщит Казахстана»: Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 (с изменениями и дополнениями от 17.03.2023 г.).

5. Алпеев А.С. Терминология безопасности: кибербезопасность, информационная безопасность. // Вопросы кибербезопасности. – 2014. - 5 (8).

6. Аверченков В.И. Системы защиты информации в ведущих зарубежных странах – М.: ФЛИНТА, 2011. – 224 с.

7. Безкоровайный М.М., Татузов А.Л. Кибербезопасность подходы к определению понятия. // Вопросы кибербезопасности. – 2014. - 1 (2).

8. Бураева Л.А. О некоторых вопросах обеспечения кибербезопасности в современных условиях. // Теория и практика общественного развития. – 2015. - 13.

9. Галатенко В.А. Основы информационной безопасности. Интернет-Университет Информационных Технологий (ИНТУИТ), 2008.

10. Карасев П.А. Политика безопасности США в глобальном информационном пространстве. – Москва, 2015.

ПРАКТИЧЕСКАЯ РАБОТА №3

Тема: Пакеты антивирусных программ

Цель работы: ознакомление с основными функциями, достоинствами и недостатками современного антивирусного программного обеспечения.

Теоретическая часть

На сегодняшний день существует широкий ассортимент доступных антивирусных программ. Они отличаются как по своей цене, так и по своим функциональным возможностям. Наиболее мощные (и, как правило, более дорогостоящие) антивирусные программы на самом деле представляют собой комплекты специализированных утилит, которые, используясь совместно, обеспечивают всестороннюю защиту компьютерной системы. Большинство современных антивирусных пакетов выполняют следующие функции:

- сканирование оперативной памяти и содержимого дисков;
- непрерывное сканирование в режиме реального времени с помощью резидентного модуля;
- обнаружение аномального поведения, характерного для компьютерных вирусов;
- блокирование и/или удаление обнаруженных вирусов;
- восстановление зараженных информационных объектов;
- принудительная проверка компьютеров, подключенных к корпоративной сети;
- удаленное обновление антивирусного программного обеспечения и баз данных через Интернет;
- фильтрация сетевого трафика для обнаружения вирусов в передаваемых программных приложениях и документах;
- обнаружение потенциально опасных Java-апплетов и модулей ActiveX;
- ведение журналов, содержащих информацию о событиях, связанных с антивирусной защитой и другими функциями.

Задание:

1. Подготовить краткий доклад по заданному вопросу (см. таблица 2), используя любые доступные источники информации.

Оформить согласно следующей структуре:

1. Титульный лист
2. Содержание
3. Практическое задание
4. Таблица «Пакеты антивирусных программ»
5. Выводы

Рекомендация: Собранный материал будет наиболее актуальным, если включить в него данные, полученные практическим путем. Для этого при

возможности, установите демонстрационную версию заданного пакета ПО и протестируйте ее в течении нескольких дней.

2. Заполнить таблицу «Пакеты антивирусных программ» на основе подготовленного материала, а также докладов других студентов.

Таблица 2. Пакеты антивирусных программ.

№	Пакет антивирусного ПО	Основные функции	Достоинства	Недостатки
1	Антивирус Касперского			
2	Антивирус Dr.Web для Windows			
3	Panda Antivirus			
4	ESET NOD32 Антивирус			
5	Avast! Free Antivirus			
6	Avira AntiVir Personal			
7	Norton AntiVirus			
8	Trend Micro Internet Security			
9	Microsoft Security Essentials			
10	McAfee VirusScan			

Список использованной литературы:

1. О ратификации Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в области обеспечения информатизационной безопасности: Закон Республики Казахстан от 3 мая 2018 года.

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

3. Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности: Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 (с изменениями и дополнениями от 10.02.2023 г.).

4. Об утверждении Концепции кибербезопасности «Киберщит Казахстана»: Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 (с изменениями и дополнениями от 17.03.2023 г.).

5. Алпеев А.С. Терминология безопасности: кибербезопасность, информационная безопасность. // Вопросы кибербезопасности. – 2014. -5 (8).

6. Аверченков В.И. Системы защиты информации в ведущих зарубежных странах. – М.: ФЛИНТА, 2011. – 224 с.

ПРАКТИЧЕСКАЯ РАБОТА №4

Тема: Информационная безопасность организации

Цель работы: развить навыки и знания в области информационной безопасности и применить их на практике в рамках организации.

Задание:

1. *Изучение политики информационной безопасности:*

Изучите политику информационной безопасности вашей организации или создайте ее, если она отсутствует. Определите основные принципы и требования информационной безопасности, а также процедуры для защиты информации. Создайте обучающий материал или презентацию, объясняющую эти принципы и требования.

2. *Аудит информационной безопасности:*

Проведите аудит безопасности информационной системы в вашей организации. Используйте шаблон аудита или методику, чтобы проверить системы, процессы и политики на соответствие стандартам безопасности. Определите обнаруженные уязвимости и риски, и разработайте план мероприятий по устранению этих проблем.

3. *Тестирование на проникновение:*

Проведите тестирование на проникновение в вашу информационную систему. Можете использовать специализированные инструменты и методики для обнаружения уязвимостей и проверки защиты системы. Определите найденные уязвимости и разработайте план действий для их устранения.

4. *Обучение сотрудников:*

Подготовьте обучающую программу по информационной безопасности для сотрудников вашей организации. Включите основные принципы безопасности, методы защиты информации, правила использования паролей и сетевых ресурсов, а также приемы предотвращения фишинговых атак и социальной инженерии. Проведите тренинги или вебинары, чтобы обучить сотрудников эффективным практикам безопасности.

5. *Разработка плана реагирования на инциденты:*

Создайте план реагирования на информационные инциденты для вашей организации. Определите шаги, которые необходимо предпринять в случае нарушения безопасности, включая обнаружение, реагирование, восстановление и усиление мер безопасности. Проведите симуляцию инцидента, чтобы проверить эффективность плана и подготовленность персонала.

6. *Оценка рисков безопасности:*

Проведите оценку рисков безопасности в вашей организации. Определите ценные активы, угрозы, уязвимости и вероятность их реализации, а также потенциальные последствия. Разработайте план по управлению рисками, включающий меры для снижения рисков и мониторинг их состояния.

Примечание: Важно помнить, что при выполнении данных заданий

необходимо соблюдать правила и политики вашей организации, а также соблюдать законодательство в области информационной безопасности.

Список литературы

1. О ратификации Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в области обеспечения информатизационной безопасности: Закон Республики Казахстан от 3 мая 2018 года;

2. Указ Президента Республики Казахстан от 14 ноября 2011 года № 174 «О Концепции информационной безопасности Республики Казахстан до 2016 года»

3. Постановление Правительства Республики Казахстан «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности» от 20 декабря 2016 года № 832 (с изменениями и дополнениями от 10.02.2023г.).

4. Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 «Об утверждении Концепции кибербезопасности («Киберщит Казахстана») (с изменениями и дополнениями от 17.03.2023г.);

5. Алпеев, Анатолий Степанович. "Терминология безопасности: кибербезопасность, информационная безопасность" Вопросы кибербезопасности 5 (8) (2014).

6. Аверченков В.И. Системы защиты информации в ведущих зарубежных странах – М.: ФЛИНТА, 2011. – 224 с.

СПИСОК ЛИТЕРАТУРЫ

Нормативные правовые акты:

1. Конституция Республики Казахстан: принята 30 августа 1995 года (с изменениями и дополнениями от 01.01.2023 г.)
2. О национальной безопасности: Закон Республики Казахстан от 6 января 2012 года (с изменениями и дополнениями от 26.02.2023 г.).
3. Об информатизации: Закон Республики Казахстан от 24 ноября 2015 года (с изменениями и дополнениями от 19.04.2023 г.).
4. Об электронном документе и электронной цифровой подписи: Закон РК от 7 января 2003 г. № 370-II // Каз. правда. - 2003. - 10 янв. (с изменениями и дополнениями от 19.04.2023 г.).
5. О ратификации Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в области обеспечения информатизационной безопасности: Закон Республики Казахстан от 3 мая 2018 года.
6. О Концепции информационной безопасности Республики Казахстан до 2016 года: Указ Президента Республики Казахстан от 14 ноября 2011 года № 174.
7. Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности: Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 (с изменениями и дополнениями от 10.02.2023 г.).
8. Об утверждении Концепции кибербезопасности «Киберщит Казахстана»: Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 (с изменениями и дополнениями от 17.03.2023 г.).
9. Алгоритм формирования и использования Интегрированного банка данных Министерства внутренних дел Республики Казахстан: Приказ МВД Республики Казахстан от 14 сентября 2022 года № 747.
10. Об утверждении Правил приема и регистрации заявления, сообщения или рапорта об уголовных правонарушениях, а также ведения Единого реестра досудебных расследований: Приказ Генерального Прокурора Республики Казахстан от 19 сентября 2014 года № 89.
11. О распределении функций по ведению Единого реестра досудебных расследований в органах внутренних дел: Приказ Министерства внутренних дел Республики Казахстан от 30 декабря 2014 года № 960.

Основная:

12. Аверченков В.И. Системы защиты информации в ведущих зарубежных странах – М.: ФЛИНТА, 2011. – 224 с.
13. Алпеев А.С. Терминология безопасности: кибербезопасность, информационная безопасность. // Вопросы кибербезопасности. – 2014. -5 (8).
14. Федотов Н.Н. Форензика - компьютерная криминалистика. - Москва, 2007.

15. Безкоровайный М.М., Татузов А.Л. Кибербезопасность подходы к определению понятия. // Вопросы кибербезопасности. – 2014. -1 (2).

16. Бураева Л.А. О некоторых вопросах обеспечения кибербезопасности в современных условиях. // Теория и практика общественного развития. – 2015. - 13.

17. Галатенко В.А. Основы информационной безопасности. Интернет-Университет Информационных Технологий (ИНТУИТ), 2008.

18. Карасев П.А. Политика безопасности США в глобальном информационном пространстве. – Москва, 2015.

19. Старовойтов А.В. Кибербезопасность как актуальная проблема современности. // Информатизация и связь. – 2011. – 6.- С. 4-7.

20. Сырбу А.В. Процессуальный порядок получения и использования информации с технических каналов связи в уголовном судопроизводстве: дис. канд. юрид. наук. — Караганда, 2005;

21. Анин Б.Ю. Защита компьютерной информации. — СПб.: БХВ-Петербург, 2000. - 384 с.

22. Аманов Ж.К. О некоторых вопросах уголовной ответственности за неправомерный доступ к компьютерной информации // Свобода слова и информационная безопасность государства, общества, личности: сб. матер. межд. конф. 1 — 2 марта 2001 г. — Алматы: Интернет трейнинг центр, 2001.

23. Компьютерное проникновение или заговор // Форпост. - 2002. - 4 июня.

24. Нугманова А. Т. (Завотпаева А.Т.) Частная жизнь граждан под наблюдением высоких технологий // Вестник Университета им. Д. Кунаева. - 2005. - № 2(15).

25. Преступления в сфере компьютерной информации: квалификация и доказывание: учеб. пособие / под ред. Ю.В. Гаврилина. - М.: ЮИ МВД РФ, 2003.

26. Гаврилин Ю.В. Расследование неправомерного доступа к компьютерной информации. - М., 2001.

27. Вечерский Д.А Шалькевич И.И. Расследование компьютерных преступлений. – Минск, 2001.

28. Нугманова А.Т. (Завотпаева А.Т.) Общие требования при реализации ОРМ на сетях телекоммуникаций // Информационно-коммуникационные технологии как основной фактор развития инновационного общества: мат-лы Международ. науч.практ. конф. - Усть-Каменогорск, 2007.

29. Комиссаров В., Гаврилов М., Иванов А. Обыск с извлечением компьютерной и информации // Законность. - 1999. - № 3. - С. 90.

30. Шурухнов Н.Г., Лучин И.Н. Методические рекомендации по изъятию компьютерной информации при проведении обыска // Информационный бюллетень Следственного комитета МВД РФ. - М., 1996. - № 4(89).

31. Нугманова А.Т. (Завотпаева А.Т.) «Перспективные» проблемы организации проведения оперативно-розыскных мероприятий на сетях телекоммуникаций Республики Казахстан // Экономика и право Казахстана. — 2005. - № 11.

32. Лучин И.Н., Желдаков А.А., Кузнецов Н.А. Взламывание парольной защиты методом интеллектуального перебора // Информатизация правоохранительных систем. - М.: Академия МВД России, 1996.

33. Крылов В.В. Расследование преступлений в сфере компьютерной информации. Криминалистика / под ред. Н.П. Яблокова. - М., 1999.

34. Скоромников К.С. Особенности расследования неправомерного доступа к компьютерной информации. Расследование преступлений повышенной общественной опасности: Пособие для следователя / под ред. Н.А. Селиванова, А.И. Дворкина. - М, 1998.

35. Кушниренко С.П., Панфилова Е.И. Уголовно-процессуальные способы изъятия компьютерной информации по делам об экономических преступлениях. - СПб., 1998.

36. Головин А.Ю., Коновалов С.И., Толстухина Т.В. Тактика осмотра и обыска по делам о преступлениях в сфере компьютерной информации: лекция. - Тула, 2002.

37. Гаврилин Ю.В. Расследование неправомерного доступа к компьютерной информации: дис.... канд. юрид. наук. - М., 2000.

38. Шевко Н.Р., Казанцев С.Я., Згадзай О.Э. Информационные технологии в юридической деятельности: учебное пособие. - Казань, 2016.

39. Тараскин М.М., Захаров А.Г., Коваленко Ю.И., Москвитин Г.И., Комплексная защита информации в организации: монография. – Москва, 2017.

Дополнительная литература:

40. Экенвайлер М. Преступная деятельность, совершаемая с использованием режима «онлайн» (Тезисы докладов на международной конференции «Проблемы борьбы с новыми видами экономических преступлений в России и США», 20-21 мая 1997 года). - Режим доступа: http://www.uic.ssu.samara.ru/~cclub/navigator/uglaw.htm.

41. Мелик Э. Компьютерные преступления. Информационно-аналитический обзор. - Режим доступа: http://www.melik.narod.ru.

42. Головин А.Ю. Криминалистическая характеристика лиц, совершающих преступления в сфере компьютерной информации. - Режим доступа: http://www.crime-research. org/library/Go Iovin.htm.

43. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. — М.: Горячая линия-Телеком, 2002.

44. Вехов В.Б. Особенности расследования преступлений, совершаемых с использованием средств электронно-вычислительной техники: учеб.-метод. пос. Изд. 2-е, доп. и испр. - М.: МЦ при ГУК и КП МВД России, 2000.

45. Назмышев Р.А. Особенности и методические проблемы расследования неправомерного доступа к компьютерной информации. — Костанай, 2000. - С. 15.

46. Осипенко М. Компьютеры и преступность // Информационный бюллетень НЦБ Интерпола в Российской Федерации. - 1994. - № 10.

47. Андрианов В.И., Бородин В.А., Соколов А.В. «Шпионские штучки» и устройства защиты объектов информации: справочное пособие. - СПб., 1996.

48. Зубаха В.С., Усов А.И., Саенко Г.В., Волков ГА., Белый С.Л., Семикалепова А.И. Общие положения по назначению и производству компьютерно-технической экспертизы: методические рекомендации. - М., 2000.

49. Особенности производства обыска при расследовании компьютерных преступлений. / М.М. Менжега. // Журнал российского права. – 2003. - N 12 декабрь. – 60 с.

50. Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений. – Москва, 2016.

51. Меллер К., Амуру А. Управление интернетом. – ОБСЕ, 2007.

Учебное издание

Бримжанова С.С.

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ДЕЯТЕЛЬНОСТИ ОВД

Учебное пособие

Печатается в авторской редакции

Подписано в печать 23.02.2024 г. Формат 60х84 $^{1}/_{16}$
Печать ризография. Объем 6,4 п.л.
Тираж 30 экз. Заказ № 12.

Отпечатано в типографии
Костанайской академии МВД РК им. Ш. Кабылбаева
г. Костанай, пр. Абая, 11.