АКАДЕМИЯ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ
ПРИ ГЕНЕРАЛЬНОЙ ПРОКУРАТУРЕ РЕСПУБЛИКИ КАЗАХСТАН

ИСМАИЛ БАҒДӘУЛЕТ

# Организационно-правовые аспекты обеспечения информационной безопасности в деятельности органов внутренних дел

Проект на соискание степени
магистра национальной безопасности и военного дела
по образовательной программе 7М12301 «Правоохранительная деятельность»
(профильное направление)

Научный руководитель:
профессор кафедры специальных
юридических дисциплин Института
послевузовского образования
Жемпиисов Н.Ш.,
кандидат юридических наук,
старший советник юстиции
_____

г. Косшы, 2024 г.

## РЕЗЮМЕ

Данное исследование посвящено всестороннему анализу организационно-правовых аспектов информационной безопасности в деятельности органов внутренних дел. Работа включает в себя детальный анализ концептуальных и теоретических основ информационной безопасности, в том числе определения ключевых понятий и разработку теоретической модели обеспечения информационной безопасности в правоохранительных органах. В значительной степени внимание уделено международному и национальному регулированию в этой сфере, основанному на анализе действующих нормативных актов и международных стандартов.

Исследование также охватывает аспекты правовой защиты информации, включая изучение законодательства, регулирующего обработку и распространение информации в рамках деятельности органов внутренних дел.

Основной упор сделан на анализ сложившихся правовых норм и практики их применения, что позволяет выявить не только сильные стороны, но и возможные пробелы в законодательной базе.

Кроме того, автор особое внимание уделяет методам повышения квалификации сотрудников органов внутренних дел в области информационной безопасности, включая разработку и внедрение целевых учебных программ и тренингов. Рассматривается также создание и функционирование ведомственных центров реагирования на компьютерные инциденты (CERT/CSIRT).

Магистерский проект состоит из введения, двух разделов, включающих в себя шесть подразделов, заключения, списка использованных источников и приложений. Объем работы составляет 48 печатных листов.

## ТҮЙІНДЕМЕ

Бұл зерттеу Ішкі істер органдарының қызметіндегі ақпараттық қауіпсіздіктің ұйымдық-құқықтық аспектілерін жан-жақты талдауға арналған. Жұмыс ақпараттық қауіпсіздіктің тұжырымдамалық және теориялық негіздерін егжей-тегжейлі талдауды, оның ішінде негізгі ұғымдарды анықтауды және құқық қорғау органдарында ақпараттық қауіпсіздікті қамтамасыз етудің теориялық моделін әзірлеуді қамтиды. Қолданыстағы нормативтік актілер мен халықаралық стандарттарды талдауға негізделген осы саладағы халықаралық және Ұлттық реттеуге көп көңіл бөлінеді.

Зерттеу сонымен қатар ақпаратты құқықтық қорғаудың аспектілерін, соның ішінде ішкі істер органдарының қызметі шеңберінде ақпаратты өңдеу мен таратуды реттейтін заңнаманы зерттеуді қамтиды.

Негізгі назар қолданыстағы құқықтық нормалар мен оларды қолдану практикасын талдауға аударылады, бұл тек күшті жақтарын ғана емес, сонымен

бірге заңнамалық базадағы мүмкін олқылықтарды да анықтауға мүмкіндік береді.

Сонымен қатар, автор мақсатты оқу бағдарламалары мен тренингтерді әзірлеу мен енгізуді қоса алғанда, ақпараттық қауіпсіздік саласындағы ішкі істер органдары қызметкерлерінің біліктілігін арттыру әдістеріне ерекше назар аударады. Сондай-ақ, компьютерлік инциденттерге жауап беретін ведомстволық орталықтарды (CERT/CSIRT) құру және олардың жұмыс істеуі қарастырылуда.

Магистрлік жоба кіріспеден, алты бөлімнен тұратын екі бөлімнен, қорытындыдан, пайдаланылған көздер тізімінен және қосымшалардан тұрады. Жұмыс көлемі 48 баспа парағын құрайды.

## RESUME

This study is devoted to a comprehensive analysis of the organizational and legal aspects of information security in the activities of internal affairs agencies. The work includes a detailed analysis of the conceptual and theoretical foundations of information security, including the definition of key concepts and the development of a theoretical model for ensuring information security in law enforcement agencies. Much attention is paid to international and national regulation in this area, based on an analysis of existing regulations and international standards.

The study also covers aspects of the legal protection of information, including the study of legislation governing the processing and dissemination of information within the framework of the activities of internal affairs agencies.

The main focus is on the analysis of established legal norms and the practice of their application, which allows us to identify not only strengths, but also possible gaps in the legislative framework.

In addition, the author pays special attention to methods of professional development of employees of internal affairs bodies in the field of information security, including the development and implementation of targeted training programs and trainings. The creation and operation of departmental computer incident response centers (CERT/CSIRT) is also being considered.

The master's project consists of an introduction, two sections, including six subsections, a conclusion, a list of used sources and applications. The volume of work is 48 printed sheets.

СОДЕРЖАНИЕ

# ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

УК РК – Уголовный кодекс Республики Казахстан;
ЕИС – Единая информационная система;
МВД – Министерство внутренних дел Республики Казахстан;
ОВД – Органы внутренних дел Республики Казахстан;
ИС – Информационная система;
ООН – Организация объединенных наций;
ОЭСР - Организация экономического сотрудничества и развития;
SIEM - Система управления событиями и инцидентами безопасности;
США – Соединенные Штаты Америки;
РК – Республика Казахстан.

# ВВЕДЕНИЕ

Актуальность проводимого исследования. В современном мире, где информационные технологии играют ключевую роль в развитии всех сфер общественной жизни, вопросы информационной безопасности приобретают особую актуальность.

Это особенно важно для органов внутренних дел (далее - ОВД), которые несут ответственность за поддержание общественного порядка и безопасности граждан.

Информационная безопасность в деятельности ОВД охватывает широкий спектр вопросов, начиная от защиты персональных данных граждан и заканчивая предотвращением угроз национальной безопасности, связанных с киберпространством.

Угрозы варьируются от несанкционированного доступа и распространения конфиденциальной информации до целенаправленных кибератак на информационные системы, что может иметь серьезные последствия для национальной безопасности и общественного порядка.

Тем не менее, несмотря на значительные усилия, направленные на укрепление информационной безопасности, существующие меры защиты зачастую оказываются недостаточными для противодействия постоянно развивающимся и усложняющимся угрозам, что делает актуальным поиск новых подходов и решений в области организационного и правового регулирования информационной безопасности в деятельности ОВД.

Следовательно актуальность данной темы обусловлена растущим числом угроз информационной безопасности, которые становятся всё более сложными и изощрёнными. При этом от органов внутренних дел требуется не только применения современных технологических средств защиты, но и разработки эффективной правовой базы, а также организации внутренних процессов для обеспечения высокого уровня информационной безопасности.

Кроме того, актуальность темы подчеркивается и международным контекстом. В условиях глобализации информационного пространства вопросы информационной безопасности становятся предметом внимания множества международных организаций и форумов.

Разработка и реализация международных стандартов и норм в области информационной безопасности требуют адаптации национального законодательства и практики его применения, что также акцентирует внимание на необходимости комплексного исследования данной проблематики.

Дополнительный аспект актуальности исследования связан с необходимостью обеспечения баланса между мерами по защите информации и соблюдением прав и свобод граждан, включая право на неприкосновенность частной жизни и защиту персональных данных.

Все это требует тщательного анализа правовых и организационных механизмов обеспечения информационной безопасности и разработки таких

подходов, которые позволят эффективно реагировать на угрозы без нарушения основных прав и свобод человека.

Таким образом, актуальность данной диссертационной работы обусловлена не только растущими вызовами и угрозами в области информационной безопасности, но и необходимостью разработки новых организационных и правовых механизмов защиты информации в деятельности органов внутренних дел, адаптированных к условиям цифровой экономики и информационного общества.

Оценка современного состояния решаемой практической задачи. Текущее состояние научных исследований в области информационной безопасности в деятельности органов внутренних дел требует более глубокого и всестороннего подхода к изучению.

Несмотря на существующие работы таких ученых, как Н.И. Журавленко, О.В. Тутова, А.А. Страхов, Е.А. Слесарева и И.Ю. Шорин, необходимость в дополнительных исследованиях остается актуальной. Эти исследователи уже внесли значительный вклад в разработку теоретических и практических аспектов информационной безопасности, но для комплексного понимания и развития данной темы требуются новые подходы и идеи.

К их числу можно добавить работы других значимых ученых в этой области, таких как В.Г. Киселев, который занимался вопросами защиты информации в информационно-телекоммуникационных системах, и М.С. Лебедева, исследующего проблемы кибербезопасности в государственных органах.

Также стоит упомянуть Д.А. Богатырева, который фокусируется на проблемах реализации информационной безопасности в условиях цифровизации общества.

Исследования в данной области могут включать анализ зарубежного опыта, который помог бы выявить и адаптировать лучшие практики и технологии, успешно применяемые за рубежом. Примером могут служить работы американских и европейских специалистов, таких как Брюс Шнайер, известный своими работами по криптографии и компьютерной безопасности, и Росс Андерсон, профессор из Кембриджа, который занимается вопросами безопасности данных.

Таким образом, для более полного понимания и разработки эффективных решений в области информационной безопасности органов внутренних дел необходимо сочетание теоретических исследований и практического анализа, включая изучение международного опыта и адаптацию успешных зарубежных практик.

Цель данного магистерского проекта заключается в комплексном анализе организационно-правовых аспектов обеспечения информационной безопасности в деятельности органов внутренних дел, а также в разработке предложений по совершенствованию существующей системы на основе изучения национального и международного опыта.

Для достижения поставленной цели в магистерском проекте решаются следующие задачи:

1) исследование национального и международного законодательства, регулирующего вопросы информационной безопасности;

2) анализ существующих организационных механизмов обеспечения информационной безопасности в органах внутренних дел;

3) выявление основных проблем и недостатков в действующей системе обеспечения информационной безопасности;

4) разработка практических рекомендаций по улучшению механизмов обеспечения информационной безопасности на основе анализа национального и международного опыта.

Объектом исследования в данной работе являются методы и процессы обеспечения информационной безопасности в структурах органов внутренних дел, включающие в себя не только анализ систем защиты информации, применяемых для профилактики, выявления и нейтрализации угроз безопасности информационных ресурсов, но и оценку эффективности механизмов управления и контроля за выполнением норм и стандартов информационной безопасности в данных органах.

Следовательно исследование направлено на выявление слабых мест в существующих подходах и разработку предложений по их усовершенствованию, с целью повышения общей защищенности информационных систем органов внутренних дел.

Предметом исследования являются организационные методы и технологические подходы к обеспечению информационной безопасности в структурах органов внутренних дел. В рамках данной работы анализируются специфические инструменты и процедуры, используемые для защиты информационных систем, особенности применения политик информационной безопасности и методы повышения квалификации сотрудников в этой сфере.

Особое внимание уделяется исследованию влияния внедрённых мер безопасности на уровень защиты информационных активов, а также разработке предложений по оптимизации и усовершенствованию действующих систем и процедур информационной безопасности в органах внутренних дел.

Методы и методологические основы проведения исследования. Методологическую основу исследования составляют общенаучные методы познания (анализ, синтез, сравнение, обобщение), а также специальные методы, применяемые в юридических и социологических исследованиях, включая нормативно-правовой и сравнительно-правовой анализ, экспертные оценки и анкетирование.

Обоснование научной новизны исследования. Научная новизна данного исследования заключается в разработке эффективных методов и практических решений для улучшения системы информационной безопасности в органах внутренних дел, включая внедрение передовых технологий и обучение

персонала, а также адаптацию международных стандартов к национальным условиям.

Практические рекомендации, выносимые на защиту.

1. Создание единой централизованной системы обеспечения информационной безопасности МВД.

Данное предложение направлено на интеграцию всех существующих и разрабатываемых информационных систем Министерства внутренних дел Республики Казахстан в единую защищенную сетевую структуру. Цель такой системы – обеспечить централизованный контроль, управление доступом и мониторинг всех информационных потоков внутри органа для предотвращения утечек данных, атак и других угроз безопасности. Она также включает в себя стандартизацию процедур безопасности, обучение сотрудников единым методам работы с конфиденциальной информацией и реализацию современных технологических решений для защиты информационной инфраструктуры.

2. Введение системы постоянного мониторинга и контроля соблюдения требований информационной безопасности путем внедрения современных средств защиты информации и систем.

Данное предложение представляет собой комплексную стратегию, направленную на укрепление информационной безопасности, связанной с обновлением антивирусных программ и систем предотвращения вторжений для защиты от новейших угроз, использованием передовых технологий шифрования данных для защиты конфиденциальной информации, а также применением многофакторной аутентификации для усиления защиты от несанкционированного доступа.

Кроме того, развертывание сетевых экранов нового поколения и систем управления доступом на основе ролей и полномочий сотрудников позволяет создать многоуровневую защитную систему. Эти меры способствуют созданию эффективной и адаптируемой к изменениям киберугроз защитной инфраструктуры, которая обеспечивает надежную защиту информационных активов в условиях постоянно развивающейся информационной среды.

3. Повышение квалификации сотрудников ОВД в области информационной безопасности.

Данное предложение является критически важным аспектом для обеспечения защиты информационных систем и данных, предусматривающим разработку и реализацию учебных программ, которые охватывают последние тенденции в сфере кибербезопасности, технологии защиты данных, а также методы предотвращения и реагирования на киберугрозы. Для эффективности принимаемых мер обучение должно проводиться регулярно, чтобы сотрудники могли своевременно реагировать на постоянно изменяющиеся вызовы в области информационной безопасности. Комплексный подход к обучению включает теоретические и практические занятия, а также моделирование различных сценариев угроз для повышения готовности персонала эффективно противостоять кибератакам.

Апробация и внедрение результатов. Апробация работы и ее научная значимость подтверждаются участием автора в научных конференциях, семинарах и круглых столах, посвященных вопросам информационной безопасности, а также публикациями в специализированных научных журналах.

Результаты данного исследования могут найти применение в процессе разработки и реализации стратегических и оперативных планов по обеспечению информационной безопасности в органах внутренних дел, а также при формировании методических и обучающих программ для сотрудников данных органов (приложение).

Магистерский проект подготовлен на кафедре специальных юридических дисциплин и включает в себя введение, два раздела, разделенных на подразделы, заключение, список использованной литературы и приложение.

В первом разделе на основе анализа национального и международного законодательства, а также научной литературы рассматриваются теоретические и правовые основы обеспечения информационной безопасности, выявляются основные принципы и подходы к регулированию данной сферы в различных странах.

Особое внимание уделяется анализу международного опыта и его применимости в контексте казахстанской правовой системы.

Второй раздел посвящен исследованию организационных и практических аспектов обеспечения информационной безопасности в деятельности органов внутренних дел.

В ней анализируются существующие механизмы предотвращения и реагирования на инциденты информационной безопасности, рассматривается роль обучения и повышения квалификации сотрудников в укреплении информационной безопасности, а также формулируются практические рекомендации по совершенствованию действующей системы.

Заключение суммирует основные результаты исследования, подчеркивая его теоретическую и практическую значимость. В нем также обозначаются перспективы дальнейших исследований в области обеспечения информационной безопасности в деятельности органов внутренних дел.

Таким образом, данный магистерский проект представляет собой комплексное исследование, направленное на улучшение системы обеспечения информационной безопасности в органах внутренних дел, что имеет важное значение для обеспечения национальной безопасности и защиты прав и свобод граждан в условиях информационного общества.

# 1 Правовые аспекты информационной безопасности

## 1.1 Информация и информационная безопасность

Информация – это в первую очередь знания. В современном мире она играет важную роль, предоставляя возможность в общении между людьми, организациями и государством.

Информация может иметь разные формы и представлять собой изображения, тексты, видео или аудиозаписи, а также другие типы данных, которые могут использовать для коммуникации и передачи знаний.

В эпоху цифровизации мы так или иначе сталкиваемся с беспрецедентным ростом объемов данных, которые дают толчок развитию современных технологий и методов работы с ними. Это в свою очередь способствует тому, чтобы принимались меры по эффективной защите данных, что составляет предмет информационной безопасности.

Информационная безопасность – это комплекс мер и всевозможных процессов, направленных на защиту информации от несанкционированного доступа, непреднамеренного или умышленного искажения, а также от других угроз [1].

В научной современной литературе рассматриваются разные понятия информационной безопасности, представляющей собой комплекс мер, направленных на защиту информации и информационных систем от несанкционированного доступа, и других угроз.

Некоторые авторы научных исследований такие как Франческо Сцилиро или коллектив организации NIST, подчеркивают многогранность концепции информационной безопасности, которая включает в себя конфиденциальность, целостность и доступность информации [2]. Важность интегрированного подхода к проблеме информационной безопасности связана с быстрым развитием новых технологий и ростом появляющихся угроз в цифровом пространстве, требующих адаптации и разработки современных методов защиты.

К основным принципам информационной безопасности относятся обеспечение конфиденциальности, целостности и доступности информации [3].

Конфиденциальность в первую очередь гарантирует, что доступ к информации имеют только те лица, которые имеют на это право.

Целостность подразумевает собой не просто защиту информации от каких-либо изменений или уничтожения, но и гарантирует её точность и полноту.

Доступность, как основной принцип информационной безопасности означает, что информация должна быть доступна для использования только уполномоченными пользователями и обязательно в нужное время, в нужном месте.

В настоящее время задача информационной безопасности становится наиболее важной и сложной, учитывая непрерывное развитие технологий, оборудования и увеличение количества угроз в цифровом пространстве.

Для поддержания информационной безопасности необходимо принимать комплексный подход, который включает в себя использование современных технологий и программного обеспечения для шифрования, двухфакторной аутентификации, а также регулярное обновление самого программного обеспечения и оборудования, разработку и соблюдение политик безопасности и соответствующих процедур.

Таким образом, информационная безопасность – это многогранная дисциплина, включающая в себя как физическое оборудование, так и программное обеспечение.

С развитием технологий и ростом новых киберугроз, таких как фишинг или DDoS-атаки, важность этой области постоянно возрастает.

В Казахстане информационная безопасность стала одним из приоритетных направлений в развитии цифровой экономики и общества. На сегодняшний день страна демонстрирует устойчивый прогресс в области кибербезопасности.

Согласно глобального индекса кибербезопасности Казахстан поднялся с 82-го на 31-е место, что свидетельствует о результативности многолетней работы специалистов в этой области [4].

Данные успехи стали возможными благодаря ряду мер:

- разработке концептуальных подходов к обеспечению защиты данных;
- принятию соответствующих нормативных правовых актов;
- созданию специализированных подразделений и национального координационного центра информационной безопасности.

Кроме того, в Казахстане была организована работа CERT и SOC центров, а также выделено больше грантов для исследований, что также способствовало развитию сферы информационной безопасности.

Последние отчеты в сфере обеспечения кибербезопасности в мире показывают, что Казахстан предпринимает активные шаги для усиления мер к защите информации. Важными инициативами в последнее время стали создание единой базы данных для отслеживания подозрительных финансовых операций и сертификация облачных сервисов по стандарту PCI DSS.

PCI DSS — это стандарт безопасности, который регулирует всю индустрию платежных карт. Он включает перечень необходимых процедур и политик, нацеленных на усиление безопасности транзакций, совершаемых с дебетовыми и кредитными картами, а также обеспечивает защиту держателей карт от несанкционированного доступа к их конфиденциальной информации [5].

В Казахстане также приняты меры по предотвращению продажи баз данных телефонных номеров в интернете [6].

Profit Security Day 2024 является одним из главных мероприятий Казахстана в области обеспечения информационной безопасности. Его программа охватывает самые актуальные темы:

- использование искусственного интеллекта в обеспечении кибербезопасности;
- безопасность в облачных технологиях;
- защита устройств интернета вещей;
- киберугрозы и их мониторинг, а также противодействие мошенничеству и защита данных.

Особенность данного мероприятия заключается в том, что оно проводится как в формате онлайн, так и офлайн, позволяя подключать неограниченное количество участников для широкого обмена опытом и знаниями.

Конференция еще раз подчеркивает все стремление Казахстана совершенствовать информационную безопасность, а также гибко и постепенно адаптироваться к новым вызовам цифрового века.

Проведение такого рода мероприятия демонстрирует важность сотрудничества между государством, частным сектором и неправительственными организациями для укрепления защиты в информационном пространстве.

В целях усиления этой сферы Казахстан активно развивает свою инфраструктуру безопасности, применяя различные стратегии и меры. Принятые в настоящее время шаги варьируются от законодательных до внедрения продвинутых технологических решений.

Например, создание в Казахстане единой базы данных о подозрительных финансовых операциях свидетельствует об активной роли государства в противодействии мошенничеству и отмыванию средств, в ом числе по цифровым каналам.

Международная сертификация облачных сервисов, особенно по стандартам безопасности, таким как PCI DSS, подчеркивает важность надёжной защиты данных и операций в облаке. Обеспечение безопасного хранения и обработки информации стали для нашей страны ключевым приоритетом.

Защита персональных данных, как элемент информационной безопасности также остаётся актуальной для Казахстана темой. Проблема нелегальной продажи баз данных с личной информацией требует не просто усиленного контроля, но и расследования с привлечением виновных лиц к установленной законом ответственности. Принимаемые усилия по борьбе с этим явлением, включают в себя обновление законодательства, направленое на укрепление приватности и конфиденциальности данных.

Серьёзной угрозой для безопасности становятся хакерские атаки на жизненно важные службы, такие как скорая помощь. Эти инциденты подтверждают необходимость комплексного подхода к киберзащите

критической инфраструктуры и разработки надёжных стратегий для реагирования на подобные угрозы.

На фоне глобальных киберугроз Казахстан демонстрирует комплексный и активный подход к защите национального информационного пространства.

Государство, в сотрудничестве с частными компаниями и международными партнёрами, стремится создать устойчивую цифровую среду для граждан и бизнеса.

Развивая международное сотрудничество в сфере кибербезопасности, страна подписала меморандум с Азербайджаном, что подчёркивает понимание того, что киберугрозы — это не только внутренняя проблема отдельной страны, но и глобальный вызов, требующий совместных действий на мировом уровне [7].

Казахстан делает важные шаги в укреплении национальной системы информационной безопасности, приспосабливаясь к современным киберугрозам и вызовам цифрового мира.

## 1.2 Национальный и международный опыт регулирования информационной безопасности

В условиях глобализации и цифровизации экономики информационная безопасность занимает центральное место в государственной политике многих стран. Поскольку технологии стали частью повседневной жизни, защита данных от несанкционированного доступа, изменения, раскрытия и других угроз приобретает всё большую значимость на национальном и международном уровнях.

Опыт различных государств в этой области и международное сотрудничество по вопросам информационной безопасности заслуживают особого внимания.

На национальном уровне подходы и стратегии сильно разнятся в зависимости от политической системы, уровня развития технологий и осознания актуальных угроз.

Глобальное взаимодействие в области информационной безопасности позволяет обмениваться опытом, разрабатывать стандарты и координировать усилия для более эффективного противодействия современным киберугрозам.

Казахстан уделяет большое внимание созданию надёжной законодательной и стратегической базы в области информационной безопасности.

Закон Республики Казахстан от 24 ноября 2015 года № 418-V ЗРК «Об информатизации», стал первым шагом в системном регулировании этой сферы, определив правовые основы создания, эксплуатации и защиты информационных ресурсов.

После этого законодательная база расширилась, включая специализированные законы о защите персональных данных, что обеспечило

регулирование хранения и обработки информации о личности в цифровой среде.

В 2017 году Казахстан утвердил концепцию кибербезопасности, которая нацелена на стратегическое планирование мер по укреплению информационной безопасности страны. Этот документ подчёркивает важность комплексного подхода, включая защиту критически важной инфраструктуры, противодействие киберпреступности и обеспечение цифровых прав граждан.

28 марта 2023 года постановлением Правительства Республики Казахстан № 269 утверждена Концепция цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023 – 2029 годы.

Эта концепция направлена на создание прочной цифровой инфраструктуры, адаптацию экономики и общества к новым технологиям, а также укрепление кибербезопасности на национальном уровне. Документ призван определить стратегические направления, задачи и меры по достижению этих целей

Для эффективной защиты информационного пространства в Казахстане сформирована специальная институциональная структура. Ведущую роль в координации действий на национальном уровне играет Комитет информационной безопасности, находящийся в структуре Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан. Помимо этого, другие министерства и ведомства страны создали собственные специализированные подразделения, занимающиеся информационной кибербезопасностью в рамках своей компетенции.

Страна активно внедряет современные технологии для укрепления информационной безопасности, развивая системы обнаружения и предотвращения кибератак. Кроме того, на национальном уровне созданы центры реагирования на инциденты в киберпространстве (CERT), что позволяет своевременно выявлять и нейтрализовать киберугрозы, минимизируя их возможные последствия.

Осознавая важность квалифицированных специалистов в области информационной безопасности, Казахстан уделяет большое внимание образовательным программам и курсам повышения квалификации. В стране действуют специализированные учебные программы в вузах и колледжах, а также курсы и тренинги от частных образовательных организаций и международных партнеров. Это способствует подготовке высококвалифицированных кадров, способных эффективно решать задачи в области информационной безопасности.

Опыт Казахстана в области регулирования информационной безопасности демонстрирует пример комплексного подхода к решению задач в этой важной сфере. Сочетание эффективного законодательства, развития институциональной структуры, внедрения современных технологий, подготовки квалифицированных кадров и активного международного

сотрудничества позволяет стране успешно противостоять вызовам информационной безопасности и обеспечивать защиту своего информационного пространства.

Учитывая трансграничный характер информационных угроз, международное сотрудничество в этой области становится необходимостью.

Казахстан признает важность международного сотрудничества в сфере информационной безопасности и активно работает с международными организациями и партнерами. Участие в международных программах и проектах, а также обмен опытом и лучшими практиками с другими странами позволяют Казахстану повышать эффективность своей системы информационной безопасности и способствуют укреплению глобальной киберустойчивости.

Международное сотрудничество в области информационной безопасности осуществляется через ряд глобальных и региональных организаций, а также двусторонние и многосторонние соглашения.

Будапештская конвенция о киберпреступности (2001 год), представляет собой первый международный договор, направленный на борьбу с интернет преступностью путем гармонизации национального законодательства стран-участников, улучшения механизмов международного сотрудничества и защиты прав человека в киберпространстве.

Генеральная Ассамблея ООН и ее подразделения регулярно рассматривают вопросы кибербезопасности, призывая все страны к укреплению международного сотрудничества в данной области и разработке общих подходов поведения в киберпространстве.

Европейский Союз также принимает усиленные меры по борьбе с киберпреступностью, путем активной разработки и внедрения общих стратегий и программ, направленных на повышение уровня кибербезопасности как внутри союза, так и за ее пределами. Одним из таких документов служит Директива о мерах для обеспечения высокого общего уровня безопасности сетей и информационных систем (NIS Directive).

Различные страны в этой области разрабатывают и в последующем реализуют свои национальные стратегии информационной безопасности, учитывая специфику своего информационного пространства и уровня возможных угроз внутри страны.

В Соединенных Штатах, также, как и в других странах имеется своя американская стратегия кибербезопасности, которая направлена на защиту критической инфраструктуры, предотвращение киберпреступлений и развитие международного сотрудничества в данной области.

В США действует ряд законодательных актов, направленных на обеспечение информационной безопасности. К ним относятся:

- Закон о национальной безопасности (National Security Act);

- Закон о защите инфраструктуры критического значения (Critical Infrastructure Protection Act);

- множество стратегических документов, такие как Национальная стратегия защиты киберпространства.

Российская Федерация также принимает всевозможные меры для обеспечения безопасности своего информационного пространства. Одним из важных шагов в этой области стало принятие в 2000 году Концепции национальной безопасности, где сфера информационной безопасности определена одной из приоритетных направлений.

Кроме того, в России имеются различные федеральные законы и нормативные акты, направленные на защиту информационного пространства.

Заслуживает внимание опыт Сингапура в обеспечении информационной безопасности. Это одна из стран, которая признана наиболее защищенной от различных киберугроз благодаря своей национальной стратегии кибербезопасности. Ключевым элементом данной стратегии является создание Национального агентства кибербезопасности и активное сотрудничество государства с частным сектором.

Немаловажную роль в регулировании информационной безопасности играют международные организации, такие как Организация объединенных наций, Международный союз электросвязи (ITU), Организация экономического сотрудничества и развития (ОЭСР) и другие.

Данные организации занимаются не просто разработкой соответствующих рекомендаций, стандартов или принципов в области информационной безопасности, но также способствуют обмену профессиональным опытом и информацией между государствами. Они организуют по всему миру международные конференции и семинары по вопросам кибербезопасности и борьбы с киберпреступностью.

Такое международное сотрудничество играет ключевую роль в повышении квалификации специалистов в данной области, обмене опытом, технологиями, а также лучшими практиками.

Данный подход к решению проблем информационной безопасности позволяет совершенствовать национальное законодательство каждой страны, создавать эффективные национальные и международные механизмы, а также активно сотрудничать и обмениваться опытом между странами.

Тем самым, адаптация лучших практик и международных стандартов, значительно повышает эффективность национальных систем обеспечения информационной безопасности и способствует созданию устойчивого и безопасного киберпространства.

Исходя из вышеизложенного, можно сделать вывод, что как на национальном, так и на международном уровнях принимаются значительные усилия для обеспечения информационной безопасности.

Различия в подходах к регулированию этой сферы в разных странах обусловлены множеством факторов, включая специфику национального законодательства, политическую волю, уровень технологического развития и восприятие угроз в информационном пространстве.

В то же время, международное сотрудничество и обмен опытом в области информационной безопасности способствуют разработке общих подходов и стандартов, что является ключевым фактором в борьбе с глобальными угрозами в киберпространстве.

## 1.3 Правовые аспекты обработки и защиты информации

В современном мире, где информация становится одним из основных активов для организаций и индивидов, правовые аспекты её обработки и защиты приобретают ключевое значение.

Правовое регулирование в этой сфере не только обеспечивает защиту данных от несанкционированного доступа, изменения, использования или уничтожения, но и способствует формированию информационного общества, базирующегося на доверии, безопасности и уважении частной жизни.

На международном уровне приняты документы, устанавливающие принципы обработки и защиты данных. Важные среди них:

- общий регламент по защите данных, введённый Европейским Союзом, предъявляющий строгие требования к обработке персональных данных, позволяя людям лучше контролировать свои личные данные [8];

- Конвенция 108 Совета Европы о защите лиц в контексте автоматизированной обработки персональных данных, которая стала первым международным договором, гарантирующим права человека при обработке данных [9, 2].

На национальном уровне каждая страна разрабатывает свои законы по обработке и защите данных в соответствии с международными стандартами, учитывая специфику местного информационного пространства.

Примеры национального законодательства включают:

- Закон Республики Казахстан от 21 мая 2013 года № 94-V ЗРК «О персональных данных и их защите», который устанавливает правила сбора, обработки, хранения и передачи личной информации. Он обеспечивает защиту прав и свобод человека, оберегая его персональные данные.

- Концепция кибербезопасности от 30 июня 2017 года, нацеленная на защиту критически важной информационной инфраструктуры и укрепление безопасности страны в цифровой среде.

Правовое регулирование в сфере информационной безопасности включает несколько ключевых компонентов:

- конфиденциальность информации *(обеспечивает защиту данных от несанкционированного доступа и раскрытия)*;

- целостность информации *(предотвращает несанкционированное изменение данных)*;

- доступность информации *(гарантирует доступ уполномоченных лиц к данным в случае необходимости)*.

- защита персональных данных *(включает меры безопасности для сбора, обработки, хранения и передачи личной информации индивидов)*.

К основным и важным проблемам и вызовам правового регулирования информационной безопасности относится:

- разработка и согласование национальных, в том числе международных норм, предусматривающих гармонизацию как правовых систем, так и возможных стандартов в целях унификации подходов к безопасности информации;

- технологическое развитие сферы информационной безопасности, связанное необходимостью регулярного обновления законодательных актов государства;

- защита прав и свобод человека и гражданина.

Данные правовые аспекты защиты информации являются основой или фундаментом для безопасности общества от киберугроз. Вместе с тем, необходимо отметить, что быстрая смена современных технологий требует от всей правовой системы гибкого подхода и постепенной адаптации, что может быть достигнуто в том числе с помощью укрепления международного сотрудничества.

Особое внимание требуется уделить правовым аспектам защиты интеллектуальной собственности, в том числе в интернете.

В условиях развивающейся цифровой экономики отдельные вопросы защиты интеллектуальной собственности приобретают особую значимость и актуальность. Распространение цифровых копий произведений в интернете без согласия их правообладателей, незаконное использование патентованных технологий, а также другие формы нарушения прав интеллектуальной собственности требуют самой быстрой и адекватной реакции от государства на данные нарушения.

В этом направлении самым значимым шагом будет являться развитие механизмов цифровой идентификации авторов путем управления правами на использование их произведений.

Еще одним важным моментом обеспечения информационной безопасности является сбор и анализ больших объемов данных, которые имеют большинство организаций независимо от форм собственности. Хранение данных, являющихся персональной информацией о каждом гражданине порождает немало вопросов, связанных с правом на конфиденциальность и защиту.

Регулирование данной сферы включает в себя установление конкретных правил, регулирующих вопросы сбора, хранения и обработки данных, обеспечения прозрачности их использования и предоставление другим пользователям в целях контроля над их персональной информацией.

Следует также отметить, что развитие информационных технологий привело к появлению такого вида уголовного правонарушения как киберпреступление.

Правовое регулирование в этой области связано с определением и классификацией таких преступлений, в том числе установлением соответствующей ответственности граждан за их совершение, разработкой необходимых мер по их расследованию и недопущению в будущем.

Поскольку многие из этих преступлений носят трансграничный характер, то важным элементом борьбы с данным видом преступлений является международное сотрудничество, позволяющее формировать универсальные принципы и стандарты, в том числе в сфере обработки и защиты информации.

Если ранее приватность ассоциировалась преимущественно с физическим изоляционизмом и конфиденциальностью личной жизни, то в современном мире она всё чаще связана с контролем над распространением личной информации в интернете. Правовые системы сталкиваются с задачей обеспечения защиты данных граждан в условиях, когда технологические возможности их сбора и анализа растут экспоненциально.

Прогресс в развитии искусственного интеллекта и машинного обучения открывает новые возможности для анализа и использования больших данных.

Однако это также порождает правовые вызовы, связанные с необходимостью обеспечения прозрачности алгоритмов и предотвращения дискриминации.

Регулирование использования ИИ для обработки персональных данных требует разработки новых подходов, способных гарантировать соблюдение прав и свобод человека.

Социальные сети стали неотъемлемой частью жизни современного человека, но их использование порождает риски для приватности.

Пользователи часто не полностью осознают масштаб информации, которой они делятся в интернете, а также возможные последствия такого обмена.

Для решения этой проблемы важны правовые механизмы, которые обязывают операторов социальных сетей надёжно защищать данные пользователей и информировать их о возможных рисках и последствиях.

Анонимность в интернете и право на забвение – ключевые аспекты защиты конфиденциальности. Право на забвение даёт пользователям возможность требовать удаления своих данных из поисковых систем, если информация устарела или нарушает их права [10]. Государства должны вводить законы и контролировать их соблюдение, чтобы обеспечить реализацию этого права.

Поскольку интернет глобален, защита конфиденциальности требует международного сотрудничества. Важные элементы этого процесса – разработка и применение международных стандартов защиты данных, обмен лучшими практиками между странами и согласование усилий в борьбе с трансграничными киберугрозами.

В условиях стремительного развития технологий и меняющихся социальных практик постоянный диалог между государственными органами,

бизнесом, академическим сообществом и общественностью необходим для формирования надёжной системы защиты данных в интернете.

Облачные технологии полностью меняют способы хранения, обработки и передачи данных, предлагая пользователям гибкие и масштабируемые решения.

Однако такие изменения также создают новые проблемы для правового регулирования, особенно в области защиты персональных данных и конфиденциальности. Правовая база должна учитывать особенности облачных сервисов, такие как вопросы юрисдикции и трансграничной передачи данных, обеспечивая надежную защиту размещенной информации.

Интернет вещей (IoT) объединяет множество устройств, которые собирают, обрабатывают и обмениваются данными [11]. Несмотря на потенциал повышения качества жизни, он несет и риски для конфиденциальности.

Устройства IoT могут собирать обширные данные без явного согласия пользователей. Для регулирования IoT необходимо разработать специальные нормы, которые обеспечат безопасность и конфиденциальность в этой взаимосвязанной экосистеме.

В последнее время для идентификации и аутентификации лиц все более популярным становится использование биометрических данных, таких как отпечатки пальцев, голос и черты лица, обеспечивают не просто надежную защиту, но и одновременно представляют собой особо чувствительную информацию [12].

В этой связи, законодатель должен разработать такие нормативные правовые акты, которые смогут обеспечить строгий контроль за сбором, хранением и использованием этих данных, чтобы не допустить их несанкционированного применения и уж тем более распространения.

Еще одним важным механизмом для защиты персональных данных является анонимизация и псевдонимизация, которые позволяют обрабатывать информацию так, чтобы невозможно было ее идентифицировать без каких-либо дополнительных сведений [13].

Законодательство в первую очередь должно поощрять внедрение таких технологий и в свою очередь гарантировать человеку, что все его личные данные надежно защищены. То есть процессы анонимизации и псевдонимизации соответствуют надежным стандартам информационной безопасности.

Эти стандарты, предоставляя высокий уровень защиты, должны учитывать и международный и национальный опыты. Приспособление национальной правовой системы к современным вызовам представляют собой сложную и необходимую задачу.

# 2 Организационные и практические аспекты информационной безопасности

## 2.1 Организация внутренних процессов по предотвращению и реагированию на инциденты

Организация внутренних процессов в целях выявления, предотвращения и реагирования на киберинциденты включает комплекс мер, направленных на снижение рисков и минимизацию последствий. Этот процесс состоит из ряда важных и необходимых элементов, связанных с разработкой политик и процедур, внедрением системы управления инцидентами, обучением сотрудников и анализом действий после киберинцидента.

Управление инцидентами строится на четких политиках и процедурах, которые определяют последовательность действий при обнаружении инцидента.

Эти документы должны содержать описание различных типов инцидентов, их классификацию, а также процедуры регистрации, оценки и разрешения. Для эффективной системы управления инцидентами необходимо использование инструментов и технологий для отслеживания и работы над инцидентами.

Команда специалистов должна быть готова оперативно реагировать на инциденты с помощью системы уведомлений и механизмов эскалации.

Обучение сотрудников о потенциальных рисках и правилах реагирования на инциденты является важным элементом предотвращения и минимизации последствий возможных происшествий. Регулярные тренинги и симуляции помогают сотрудникам лучше понять свою роль в управлении инцидентами.

После ликвидации проблемной ситуации следует провести детальный анализ причин произошедшего и оценить эффективность предпринятых мероприятий. Это позволит разработать рекомендации по усовершенствованию процедур и повышению безопасности для предотвращения подобных случаев в будущем.

Процесс управления инцидентами требует постоянного совершенствования на основе накопленного опыта, изменений в информационной обстановке и новых технологий безопасности.

Регулярное обновление политик, пересмотр процедур, модернизация технических средств и постоянное обучение персонала способствуют повышению безопасности в организации.

Для успешного предотвращения или ликвидации возможных проблем необходим комплексный подход, объединяющий технические, организационные методы со стойкой культурой безопасности всей команды.

Исходя из информации от компании Atlassian и ООН, можно заключить, что организация внутренних процессов по предотвращению и реагированию на

инциденты – это сложный процесс, требующий внимания к деталям и постоянного совершенствования [14].

Этот процесс включает в себя технические аспекты, такие как управление инцидентами и кибербезопасность, а также обучение персонала, разработку политик и процедур, анализ опыта предыдущих инцидентов и непрерывное улучшение процессов.

Современные технологические решения, такие как системы обнаружения вторжений, антивирусные программы, инструменты управления журналами событий и мониторинга сетевой активности играют ключевую роль в выявлении и предотвращении инцидентов. Их эффективное использование помогает быстро выявлять потенциальные угрозы и предотвращать нанесение ущерба.

Несмотря на прогресс технологий, человеческий фактор остается одним из основных элементов в области безопасности. Обучение персонала принципам информационной безопасности и методам борьбы социальной инженерии является крайне важным. Регулярные тренировки по реагированию на инциденты поддерживают готовность команды к действиям при нештатных ситуациях.

Эффективное управление изменениями в приложениях и IT-инфраструктуре имеет ключевое значение для обеспечения безопасности.

Каждое изменение должно быть подвергнуто формализованной проверке: оценке рисков, проверке безопасности и тщательной документации. Это поможет избежать появления потенциальных уязвимостей, которые могут быть использованы злоумышленниками.

План восстановления после инцидента необходим для оперативного возобновления работы. Планы включают в себя подробные процедуры по восстановлению данных и шаги для восстановления работоспособности сетевой инфраструктуры и других ИТ-систем.

Постоянный мониторинг безопасности с применением систем управления событиями и информацией (SIEM) позволяет объединять и анализировать логи из различных источников, выявляя аномальные и потенциально опасные события [15]. Это повышает эффективность управления инцидентами и помогает предотвращать риски.

Подход к организации внутренних процессов по предотвращению и реагированию на инциденты включает технические, организационные и образовательные компоненты. Важно осознавать, что безопасность - это непрерывный процесс, который требует регулярного обновления и приспособления к новым угрозам. Внедрение принципов безопасности в корпоративную культуру способствует созданию надежной системы защиты.

Успешное управление инцидентами во многом зависит от способности организации оперативно и эффективно реагировать, минимизируя ущерб и время простоя. Для этого необходимо не только иметь технологические решения и процедуры, но также активное участие всего персонала в

обеспечении безопасности, развитие культуры постоянного обучения и совершенствования.

Организации должны постоянно пересматривать свои подходы к безопасности с учетом актуальных угроз и быстро развивающихся технологий. Это подразумевает регулярное обновление политик безопасности, проведение аудитов и тренировок, а также инвестиции в профессиональное развитие сотрудников и модернизацию технической базы.

Создание надежной системы предотвращения и реагирования на инциденты - сложная, но значимая задача. Этого требует комплексный подход со стороны всех работников организации. Такая система позволяет не только защитить ключевые активы компании, но также повысить ее стойкость перед различными внешними или внутренними угрозами.

В условиях сотрудничества организаций со сторонними партнерами, сервис-провайдерами и облачными платформами становится все более актуальной потребность учитывать новые слабые места при управлении инцидентами. Коллаборация с другими структурами играет ключевую роль для эффективного ответа на возможные опасности и минимизации возможных потерь.

Необходимо заранее разработать и внедрить четкие соглашения о качестве обслуживания, которые определяют требования безопасности в отношениях с партнерами и распределяют ответственность.

Для более оперативного реагирования на инциденты очень важен своевременный обмен информацией о угрозах и атаках, что способствует выявлению и предотвращению нарушений.

Также необходимо разработать общую стратегию по восстановлению после инцидентов с координацией действий между организациями и внешними партнерами. В современном мире технологии искусственного интеллекта значительно расширяют возможности выявления и предотвращения киберинцидентов.

Системы на основе ИИ анализируют большие объемы данных и выявляют аномалии в поведении систем, пользователей и сетевом трафике, что позволяет оперативно реагировать на угрозы для быстрого устранения проблем. Кроме того, автоматизация повседневных задач благодаря использованию ИИ освобождает время специалистов для работы над более сложными проблемами.

Поэтому управление доступом и подтверждение личности пользователей играют ключевую роль в обеспечении безопасности. Контроль за доступом к данным помогает минимизировать потенциальные риски, повышая эффективность предотвращения инцидентов и оперативного реагирования на них.

Интеграция этих мер в единую стратегию управления инцидентами помогает организациям лучше приспосабливаться к современным киберугрозам и поддерживать стабильную систему безопасности.

В целях защиты от несанкционированного доступа злоумышленников и возможных киберинцидентов важно внедрить многофакторную аутентификацию, как элемент информационной безопасности, держать под контролем привилегированные аккаунты, постоянно пересматривать политику доступа и анализировать поведение пользователей [16].

Все это способствует выявлению нетипичных ситуаций и уменьшению рисков. Моделирование возможных инцидентов и анализ угроз позволяют компаниям определить слабые места и понять, насколько они готовы реагировать на различные ситуации. Регулярные тренировки по заданным сценариям проверяют эффективность команды в кризисных ситуациях и ее общую готовность.

Формирование культуры безопасности предполагает активное участие всех работников в процессах обеспечения сохранности данных. Проявление лидерства со стороны руководства помогает выделить необходимые ресурсы, внедрить стратегии безопасности и создать атмосферу, где защита информации становится приоритетом.

Руководители должны демонстрировать свою приверженность кибербезопасности через личный пример, поддержку образовательных программ и непрерывное развитие процессов. Организация внутренних механизмов для предотвращения инцидентов - сложная задача, требующая комплексного подхода и активного участия всех служб организации.

От использования технологических инноваций и управления доступом до обучения персонала и формирования культуры безопасности – каждый элемент играет ключевую роль в построении надежной системы защиты. Постоянное совершенствование, адаптация к новым вызовам и технологиям, активное лидерство и поддержка со стороны верхнего руководства создают основу для стойкости организации в быстро меняющемся мире информационных технологий [17].

Безопасность – это не статическое состояние, а непрерывный процесс, который требует постоянного внимания, обучения и адаптации. Эти стандарты предлагают проверенные методы и практики для эффективного управления информационной безопасностью, рисками и соответствием требованиям, что является важным для предотвращения инцидентов и минимизации их последствий.

Участие в отраслевых группах по безопасности и использование информационных платформ об угрозах позволяет организациям оперативно получать информацию о новых рисках и методах их предотвращения. Такое совместное сотрудничество способствует совместной защите от общих угроз, повышая устойчивость к кибератакам на уровне всей отрасли или региона.

Помимо технической подготовки, важную роль играют стойкость и способность команды эффективно реагировать в кризисных ситуациях. Навыки работы в команде, стрессоустойчивость и способность принимать решения под

давлением улучшают эффективность реагирования на инциденты и ускоряют процесс восстановления.

Инциденты безопасности могут серьезно повлиять на имидж организации.

Разработка стратегий по управлению имиджевыми рисками, включая коммуникационные планы для общения с клиентами, партнерами и общественностью в период кризиса, помогает сохранить доверие и сократить негативное воздействие на осознание.

Принимая в расчет множество аспектов процесса организации мероприятий по предупреждению инцидентов и ответам на них, очевидно, что подход должен быть комплексным и многослойным.

Он не только затрагивает технические решения и процедуры, но также требует интеграции элементов корпоративной культуры, психологической подготовки, стратегического планирования и координации со сторонними партнерами.

Важно также понимать, что безопасность - это не только защита от внешних угроз, но и управление внутренними рисками, подготовка к неожиданным ситуациям и способность адаптироваться и восстанавливаться после инцидентов.

Каждая организация должна стремиться к созданию системы, в которой безопасность рассматривается как непрерывный процесс, требующий постоянного внимания, инвестиций и развития.

Постоянное обучение, адаптация к новым угрозам, применение передовых технологий и поддержание культуры, в которой безопасность является общей ответственностью, помогут обеспечить устойчивость и долгосрочный успех в борьбе с киберугрозами.

Таким образом, организация внутренних процессов по предотвращению и реагированию на инциденты требует комплексного подхода, включающего в себя различные стратегии и меры на всех уровнях организации.

Успешное управление безопасностью не ограничивается одними лишь техническими средствами, но также включает в себя управленческие, организационные и культурные аспекты, обеспечивая комплексную защиту от угроз и поддержание высокого уровня готовности к реагированию на инциденты.

В деятельности органов внутренних дел защита конфиденциальной информации, поддержание общественного порядка и обеспечение национальной безопасности являются первостепенными задачами.

В связи с растущей зависимостью от информационных технологий и данных органы внутренних дел должны уделять приоритетное внимание организации эффективных внутренних процессов по предотвращению и реагированию на инциденты информационной безопасности.

Помимо общих рекомендаций, перечисленных ранее, органы внутренних дел должны учитывать и другие специфические моменты.

Усиленное сотрудничество с правоохранительными партнерами *(установление и поддержание прочных партнерских отношений с другими правоохранительными органами, а также с национальными и международными организациями по кибербезопасности)*. Это сотрудничество должно выходить за рамки обмена информацией и включать совместные расследования, скоординированные усилия по борьбе с киберпреступностью и взаимную помощь в случае крупных инцидентов информационной безопасности.

Специализированная подготовка и обучение сотрудников *(предоставление сотрудникам органов внутренних дел специализированной подготовки и обучения по вопросам реагирования на инциденты информационной безопасности, цифровой криминалистики и расследования киберпреступлений)*.

Данное обучение должно охватывать как технические аспекты, так и правовые и процедурные требования.

Использование криминалистических инструментов и технологий *(оснащение органов внутренних дел передовыми криминалистическими инструментами и технологиями)*. Такие инструменты должны позволять собирать, анализировать и сохранять электронные доказательства в случае киберпреступлений и инцидентов информационной безопасности.

Соблюдение правовых и нормативных требований *(обеспечение соответствия всем применимым правовым и нормативным требованиям, связанным с защитой данных, конфиденциальностью и реагированием на инциденты информационной безопасности)*. Включает в себя понимание и соблюдение законов о защите данных, правил обращения с электронными доказательствами и протоколов раскрытия информации.

Создание специализированных подразделений по кибербезопасности *(рассмотрение возможности создания специализированных подразделений по кибербезопасности в рамках органов внутренних дел)*. Такие подразделения должны централизовать экспертные знания и ресурсы, связанные с предотвращением и реагированием на инциденты информационной безопасности, а также выступать в качестве центра координации усилий по борьбе с киберпреступностью.

Эффективная организация внутренних процессов по предотвращению и реагированию на инциденты информационной безопасности в деятельности органов внутренних дел имеет решающее значение для защиты конфиденциальной информации, поддержания общественного порядка и обеспечения национальной безопасности в эпоху растущих киберугроз.

В условиях возрастающей зависимости от информационных технологий и данных органы внутренних дел должны уделять первостепенное внимание организации эффективных внутренних процессов по предотвращению и реагированию на инциденты информационной безопасности.

Всеобъемлющий подход к этому вопросу должен включать следующие ключевые элементы:

- разработка и внедрение всеобъемлющих политик и процедур информационной безопасности, охватывающих все аспекты защиты информации, включая физическую безопасность, контроль доступа, управление уязвимостями и резервное копирование данных;
- регулярная оценка рисков и уязвимостей информационных систем и сетей для выявления и устранения потенциальных слабых мест;
- внедрение многоуровневых систем защиты, включая брандмауэры, антивирусное программное обеспечение и системы обнаружения вторжений (IDS);
- повышение осведомленности и обучение сотрудников методам социальной инженерии, фишинга и другим распространенным киберугрозам;
- создание и регулярное обновление плана реагирования на инциденты, определяющего роли и обязанности, процедуры эскалации и шаги по реагированию на различные типы инцидентов информационной безопасности;
- учреждение круглосуточного центра мониторинга безопасности (SOC) для выявления и реагирования на инциденты информационной безопасности в режиме реального времени;
- внедрение систем управления событиями и инцидентами безопасности (SIEM) для централизованного сбора, анализа и корреляции событий безопасности;
- подготовка и проведение регулярных учений по реагированию на инциденты для проверки эффективности планов и процедур реагирования;
- установление и поддержание прочных партнерских отношений с другими правоохранительными органами, а также с национальными и международными организациями по кибербезопасности;
- активное участие в отраслевых форумах и инициативах по обмену информацией об угрозах, передовой практикой и уроками, извлеченными из инцидентов информационной безопасности;
- сотрудничество с экспертами по цифровой криминалистике и поставщиками технологий безопасности для получения поддержки в расследовании и реагировании на инциденты информационной безопасности;
- регулярный пересмотр и обновление политик, планов и процедур информационной безопасности в соответствии с меняющимися угрозами и требованиями;
- постоянное обучение и повышение квалификации сотрудников по вопросам информационной безопасности и реагирования на инциденты;
- внедрение новых технологий и передовой практики для повышения эффективности мер по предотвращению и реагированию на инциденты информационной безопасности.

Всеобъемлющий подход к организации внутренних процессов по предотвращению и реагированию на инциденты информационной безопасности

позволит органам внутренних дел эффективно противостоять постоянно растущим киберугрозам, обеспечивать конфиденциальность, целостность и доступность критически важной информации, а также поддерживать доверие общественности.

Дополнительные рекомендации по организации внутренних процессов по предотвращению и реагированию на инциденты информационной безопасности в органах внутренних дел включают:

- использование анализа поведения пользователей и сущностей (UEBA) *(внедрение UEBA для мониторинга и анализа поведения пользователей и сущностей в информационных системах для выявления подозрительной активности и предотвращения внутренних угроз)* [18];

- регулярное обновление программного обеспечения и операционных систем *(обеспечение своевременного обновления программного обеспечения и операционных систем для устранения уязвимостей и повышения общей безопасности)*.

- использование двухфакторной аутентификации (2FA) *(внедрение 2FA для добавления дополнительного уровня безопасности к процессам входа в систему и предотвращения несанкционированного доступа)* [19];

- шифрование данных в состоянии покоя и при передаче *(реализация шифрования данных в состоянии покоя и при передаче для защиты конфиденциальной информации от несанкционированного доступа и перехвата)*.

- сотрудничество с экспертами по цифровой криминалистике *(установление партнерских отношений с экспертами по цифровой криминалистике для оказания помощи в расследовании и реагировании на киберпреступления и инциденты информационной безопасности)*.

Интеграция этих дополнительных мер в общую стратегию кибербезопасности позволит органам внутренних дел еще больше укрепить свою защиту от постоянно растущих киберугроз, обеспечить целостность и конфиденциальность информации, а также быстро и эффективно реагировать на инциденты информационной безопасности.

Органы внутренних дел должны придавать первостепенное значение обучению и повышению осведомленности своих сотрудников по вопросам информационной безопасности.

Это обучение должно включать проведение регулярных тренингов и семинаров, которые нацелены на увеличение знаний о текущих угрозах и лучших практиках в области безопасности.

Также важно использовать моделирование и имитацию угроз для предоставления практического опыта в выявлении и реагировании на различные типы инцидентов.

Запуск кампаний по повышению осведомленности поможет информировать сотрудников о важности информационной безопасности и их роли в защите критически важной информации.

Все эти меры являются ключевыми элементами всесторонней стратегии по предотвращению и реагированию на инциденты информационной безопасности, и инвестиции в повышение квалификации сотрудников помогут создать более надежную и устойчивую систему информационной безопасности.

Организация внутренних процессов по предотвращению и реагированию на инциденты информационной безопасности в органах внутренних дел требует применения целостного, научно-обоснованного подхода.

Ключевым компонентом является формирование формальных процессов управления инцидентами, включая эскалацию, расследование и документирование, чтобы оперативно выявлять, анализировать и устранять проблемы.

Анализ первопричин произошедших инцидентов и реализация соответствующих корректирующих мер помогают устранить подобные уязвимости в будущем.

Соблюдение нормативных требований и отраслевых стандартов, таких как ISO 27001 и NIST Cybersecurity Framework, обеспечивает высокую степень защиты и помогает минимизировать риски.

Сотрудничество с поставщиками услуг безопасности и исследователями в данной области позволяет получить квалифицированную помощь в устранении угроз, а также обогатить собственные знания.

Непрерывный мониторинг и оценка внутренних процессов – важная составляющая обеспечения безопасности. Оперативный анализ ситуации позволяет своевременно адаптировать существующие меры и процессы к новым угрозам.

Использование технологий искусственного интеллекта и машинного обучения повышает уровень защиты за счет автоматизации рутинных задач и выявления угроз в реальном времени.

Внедрение облачных сервисов, таких как MSS (управляемые службы безопасности) и EDR *(обнаружение и реагирование на расширенные угрозы)*, дополняет внутренние возможности реагирования на инциденты.

Регулярное резервное копирование данных и детально продуманные планы восстановления позволяют организациям минимизировать потенциальные потери в случае серьезных инцидентов.

Партнерство с национальными центрами по реагированию на киберугрозы обеспечивает своевременное оповещение о возникающих угрозах и содействует координации мероприятий по их устранению.

Такой комплексный подход формирует устойчивую систему защиты, которая эффективно противостоит возникающим киберугрозам и сохраняет безопасность организации в условиях постоянно меняющегося ландшафта информационной безопасности.

Для укрепления безопасности в органах внутренних дел следует создать всестороннюю систему кибербезопасности, которая поощряет создание культуры защиты информации.

Сотрудники должны быть хорошо осведомлены о своей роли в обеспечении безопасности данных и активно участвовать в обеспечении надежной защиты.

Регулярные проверки и аудит систем позволяют оперативно выявлять слабые места и оценивать эффективность внедренных мер безопасности.

Биометрическая аутентификация, основанная на распознавании лиц или отпечатков пальцев, обеспечивает надежный способ ограничения доступа к конфиденциальной информации и системам.

Одновременно важно инвестировать в повышение квалификации сотрудников, чтобы они могли проводить цифровые расследования и реагировать на инциденты кибербезопасности.

Партнерство с академическими учреждениями обогащает внутренние ресурсы организации за счет исследований и обмена знаниями в области информационной безопасности.

Интеграция всех этих мер в стратегию информационной безопасности органов внутренних дел поможет повысить их киберустойчивость, улучшить выявление инцидентов и своевременно реагировать на них.

## 2.2 Обучение и повышение квалификации сотрудников ОВД в сфере информационной безопасности

В условиях современного мира информационная безопасность приобретает все большее значение, непосредственно влияя на национальную безопасность и общественный порядок. Это диктует необходимость в подготовке квалифицированных специалистов в сфере информационной безопасности, включая сотрудников органов внутренних дел.

В настоящее время подготовка и повышение квалификации сотрудников органов внутренних дел Казахстана в сфере информационной безопасности осуществляется в рамках следующих основных программ:

- базовое обучение *(курсанты и слушатели Академии МВД Республики Казахстан проходят обучение по дисциплине «Информационная безопасность» в рамках учебных программ по различным специальностям)*.

- профессиональная переподготовка *(сотрудники органов внутренних дел, имеющие высшее или среднее профессиональное образование в других областях, могут пройти профессиональную переподготовку по специальности «Информационная безопасность» в Академии МВД Республики Казахстана или других учебных заведениях)*.

- повышение квалификации *(сотрудники органов внутренних дел, имеющие базовое или специальное образование в сфере информационной безопасности, могут повышать свою квалификацию на курсах повышения квалификации, организуемых Академией МВД Республики Казахстан и другими учебными заведениями)*.

Кроме того, сотрудники органов внутренних дел могут проходить обучение и повышение квалификации в зарубежных учебных заведениях и на специализированных курсах, проводимых международными организациями.

Несмотря на наличие существующих программ обучения, система подготовки и повышения квалификации сотрудников органов внутренних дел Казахстана в сфере информационной безопасности имеет ряд проблем:

- недостаточное финансирование, что ограничивает возможности для организации качественной подготовки специалистов;
- устаревшие учебные программы, которые не всегда соответствуют современным требованиям и нуждаются в регулярном обновлении;
- нехватка преподавательских кадров, имеющих высокий уровень квалификации и практический опыт в сфере информационной безопасности;
- слабая материально-техническая база, необходимая для подготовки специалистов в сфере информационной безопасности;
- недостаточное внимание к практической подготовке, что снижает эффективность обучения и не позволяет выпускникам сразу приступить к выполнению служебных обязанностей в сфере информационной безопасности;
- недостаток единых стандартов и требований в подготовке специалистов по информационной безопасности приводит к неоднородности учебных программ и различиям в уровне квалификации выпускников.

Это несоответствие обусловлено разнообразием подходов к обучению и недостаточной координацией между образовательными учреждениями, что препятствует созданию единых, универсальных компетенций.

Разработка унифицированных стандартов и требований к подготовке кадров способствовала бы согласованному, эффективному развитию профессиональных навыков в этой области.

Для развития и оптимизации системы обучения сотрудников органов внутренних дел Казахстана в области информационной безопасности необходимо повысить уровень инвестиций и пересмотреть учебные программы.

В частности, важно расширить финансирование образовательных и квалификационных программ, чтобы обеспечить качественное оборудование, разработать современные учебные материалы и привлечь квалифицированных преподавателей.

Финансовая поддержка позволит совершенствовать программы, снабжая обучающихся актуальными инструментами и знаниями.

Кроме того, рекомендуется регулярно пересматривать и обновлять учебные программы, адаптируя их к актуальным требованиям и современным методикам.

Установление единых стандартов подготовки кадров поможет создать единую систему требований для обеспечения квалифицированной работы специалистов в этой области.

Такой подход обеспечит сотрудников органов внутренних дел необходимыми компетенциями и современными методами для эффективного решения задач в области информационной безопасности.

Чтобы усовершенствовать подготовку специалистов в области информационной безопасности, необходимо привлекать к преподаванию ведущих специалистов-практиков, обладающих обширным опытом, и организовывать повышение квалификации педагогов в ведущих учебных учреждениях и специализированных курсах.

Дополнительно, необходимо улучшить материально-техническую базу образовательных учреждений, оснащая их современным оборудованием и специализированными лабораториями для обеспечения высококачественной подготовки.

Особое внимание следует уделить практической части образования, что включает организацию стажировок и практик в отделах, занимающихся информационной безопасностью.

Внедрение системы непрерывного обучения позволит сотрудникам правоохранительных органов регулярно повышать свою квалификацию и переобучаться в соответствии с актуальными требованиями и технологическими достижениями.

Для повышения эффективности подготовки и профессионального развития сотрудников правоохранительных органов Казахстана в области информационной безопасности необходимо активно развивать международное сотрудничество.

Это может включать обмен опытом и передачу лучших практик, проведение совместных программ обучения и стажировок, а также привлечение международных экспертов для разработки учебных программ и преподавания.

Обучение и повышение квалификации специалистов правоохранительных органов Казахстана по информационной безопасности - это ключевая задача для гарантирования национальной безопасности и сохранения общественного порядка.

Для улучшения системы образования необходимо решить текущие проблемы, такие как недостаточное финансирование, устаревшие программы обучения, нехватка преподавателей, слабая материально-техническая база и отсутствие единого стандарта подготовки. Решение этих проблем поможет повысить качество подготавливаемых специалистом по информационной безопасности и предоставит правоохранительным органам высококвалифицированный персонал для защиты информационных систем от киберугроз.

Симуляционное тренировочное занятие является эффективным методом подготовки специалистом по информационной безопасности. Оно дает возможность студентам отработать практические навыки в усложненных условиях близко к реальным.

Обучение с использованием симуляций может включать работу в виртуальных лабораториях, имитационных системах и ролевых играх.

Внедрение такого обучения в программы для сотрудников правоохранительных органов Казахстана по информационной безопасности поможет улучшить их практическую подготовку к исполнению служебных обязанностей.

Для повышения эффективности обучения и развития профессиональных навыков сотрудников правоохранительных органов по информационной безопасности необходимо применять новейшие технологические решения.

Использование виртуальной и дополненной реальности позволяет создавать интерактивные симуляции, погружаясь в реалистичные учебные сценарии и моделируя различные инциденты, что способствует формированию навыков реагирования на угрозы.

Использование искусственного интеллекта автоматизирует анализ данных, выявление угроз, а также способствует созданию более эффективных методов защиты от киберугроз.

Применение методов работы с большим объемом данных обеспечивает глубокий анализ и прогнозирование кибератак, способствуя разработке актуальных стратегий и тактик защиты.

С использованием передовых технологий в процессе образования специалистам предоставляются необходимые знания и навыки для успешного противодействия динамично возрастающим киберугрозам.

Крайне важно также внедрить систему сертификации для оценки квалификации специалистов и подтверждения соответствия их навыков установленным стандартам, что укрепит доверие к их профессионализму, поможет государственным структурам и работодателям объективно определять квалификацию персонала и обеспечит актуальность подготовки персонала.

Подготовка и повышение квалификации работников правоохранительных органов Казахстана по информационной безопасности требуют постоянного развития и адаптации ко всё более изменчивой природе киберугроз.

Для улучшения качества подготовки специалистов и обеспечения органов внутренних дел квалифицированными кадрами необходимо установить надежную систему защиты информационных ресурсов и инфраструктуры от киберпреступности.

Кроме того, для эффективного обучения важно использовать междисциплинарный подход. Помимо технических навыков и знаний, персонал должен быть осведомлен о смежных областях, таких как правовое регулирование информационной безопасности, криминалистика в сфере информационных технологий, психология киберпреступности и управление информационными рисками. Такой комплексный подход способствует глубокому пониманию задач информационной безопасности.

Важную роль в повышении профессионального уровня сотрудников играют представители бизнеса и промышленности, которые могут делиться

знаниями, опытом и передовыми методами защиты. Это сотрудничество способствует разработке образовательных программ, соответствующих требованиям рынка труда, а также проведению практических стажировок для персонала.

Кроме того, важно развивать научные исследования в области информационной безопасности для изучения новых киберугроз и методик противодействия им, а также для постоянного совершенствования учебных материалов и методологий обучения.

Изучение передовых практик и разработка новых методик помогает постоянно улучшать систему подготовки специалистов для эффективного противодействия вызывающим изменениям в технологической среде вызовам.

Подготовка и повышение квалификации персонала органов внутренних дел по вопросам информационной безопасности представляет собой сложную задачу требующую комплексного подхода через активное сотрудничество со стороны бизнеса и промышленности, а также постоянное развитие наукой процесса.

Введение данных мер поможет создать систему образца высокого класса где будут подготавливаться высококвалифицированные специалисты способные гарантировать стабильность информационной безопасности и препятствующие нарастанию киберугроз.

При разработке и улучшении программы подготовки персонала важно учитывать международные стандарты и рекомендации, такие как серия стандартов ISO/IEC 27000 по управлению информационной безопасностью, кибербезопасностная структура NIST Cybersecurity Framework от Национального института стандартов и технологий США, а также рекомендации Европейского агентства по сетевой и информационной безопасности (ENISA).

Соблюдение этих норм позволяет привести обучение в соответствие с передовыми мировыми практиками.

Важную роль играют психологические аспекты, так как сотрудники сталкиваются с высоким уровнем стресса и необходимостью оперативных решений.

Обучающие программы должны включать тренинги по развитию стрессоустойчивости, повышению концентрации и развитию аналитического мышления в условиях неопределенности.

Этическая подготовка является неотъемлемой частью обучения.

Специалистам необходимо придерживаться высоких этических стандартов, осознавать юридические последствия своих действий и обеспечивать конфиденциальность данных. Программы обучения должны включать курсы по защите персональной информации и соблюдению законодательства.

Такая комплексная подготовка поможет сотрудникам органов внутренних дел Казахстана успешно противостоять новым киберугрозам и гарантировать надежную защиту информационных ресурсов.

Существующая система обучения и повышения квалификации в Казахстане имеет свои проблемы, такие как ограниченное финансирование, устаревшие учебные программы, недостаток опытных преподавателей и слабую материально-техническую базу.

В стране система образования персонала органов внутренних дел (ОВД) в области информационной безопасности организуется согласно национальным правилам и стандартам на государственном уровне.

Правила подготовки, переподготовки и повышения квалификации государственных служащих охватывают широкий спектр требований к учебным заведениям, которые занимаются повышением квалификации государственных служащих, включая область информационной безопасности.

Государственные служащие, включая сотрудников ОВД, имеют право на обучение по программам послевузовского образования в рамках государственного заказа.

На такое обучение допускаются госслужащие, занимающие постоянные должности в госорганах, причем учитывается продолжительность обучения и последующей работы, не превышающие установленного пенсионного возраста.

Госслужащему, направляемому на обучение, предоставляется отпуск с сохранением рабочего места. По окончании обучения госслужащим выдается документ о полном освоении профессиональной образовательной программы.

Переподготовка лиц, только что начавших работу на административной государственной службе, проводится в Академии государственного управления и ее филиалах. Здесь проходят переподготовку госслужащие различных уровней ответственности за вопросы информационной безопасности.

Специализированные курсы переподготовки предлагают разнообразные программы и методики для административных госслужащих различных рангов от Академии государственного управления.

Обучение акцентируется на компетентностях по информационной безопасности - ключевом аспекте деятельности госорганов в сегодняшнем мире.

Функциональные задачи органов внутренних дел Республики Казахстан охватывает широкий спектр функций: контроль и надзор за физическими лицами и объектами; контроль за антитеррористической безопасностью; реализация политики страны по вопросам миграции и гражданства.

Важно подчеркнуть, что сфера ответственности включает как обеспечение выполнения международных обязательств, так и международное сотрудничество, что подчеркивает важность знаний в области информационной безопасности для сотрудников органов внутренних дел.

В рамках гарантирования безопасности информации и защиты данных крайне важно, чтобы процесс обучения и повышения квалификации сотрудников ОВД регулярно соответствовал требованиям и стандартам.

В Казахстане особое внимание уделяется государственному контролю и профессиональной подготовке в области информационной безопасности, что отражается в утвержденных правилах подготовки и повышения квалификации государственных служащих.

Особое значение придаётся переподготовке тех сотрудников, которые только начинают свою службу в административных государственных учреждениях, а также тем, кто назначается на ключевые посты управления.

Процесс обучения может осуществляться различными способами: очным, онлайн или дистанционным образом.

Стоит отметить, что определённые лица, ранее занимавшие должности в правоохранительных или специализированных государственных органах, могут быть освобождены от переподготовки.

Полномочия правоохранительных органов Казахстана охватывают широкий диапазон функций: от государственного контроля и надзора до защиты объектов, и личности. Это подчёркивает значимость компетентности по информационной безопасности для эффективного выполнения своих функций.

Это не только способствует улучшению защиты государственных и личных данных, но и повышает общую устойчивость страны к киберугрозам.

Обучение и повышение квалификации сотрудников правоохранительных органов являются важными элементами национальной стратегии безопасности, направленной на защиту информации и данных граждан от киберугроз.

Регулярное обучение способствует формированию высококвалифицированных специалистов, способных обеспечивать надежную защиту информационного пространства страны.

Вклад каждого сотрудника правоохранительных органов, прошедшего соответствующее обучение, в систему информационной безопасности Казахстана нельзя переоценить.

Подготовленные эксперты не только помогают укрепить защиту от внешних и внутренних угроз, но также создают основу для развития национальных компетенций в области кибербезопасности.

Для дальнейшего изучения темы образования и повышения квалификации сотрудников правоохранительных органов по информационной безопасности в Казахстане можно обратиться к официальным ресурсам правительства РК, учебным заведениям, специализированным по подготовке в этой сфере, а также к научным и профессиональным публикациям по данной тематике.

Эти материалы предоставят более глубокое понимание текущих тенденций, методологий и лучших практик использования в сфере информационной безопасности для повышения профессионализма сотрудников

правоохранительных органов и укрепления защиты информационного пространства Казахстана.

## 2.3 Практические рекомендации по совершенствованию системы обеспечения информационной безопасности в органах внутренних дел

Обеспечение безопасности информации в органах внутренних дел играет ключевую роль в защите конфиденциальных данных, обеспечении общественного порядка и национальной безопасности.

1. Создание и внедрение единой комплексной системы защиты информации.

Путем создания централизованной системы защиты информации органы внутренних дел могут гарантировать согласованные и эффективные действия по обеспечению информационной безопасности во всех отделах.

Эта система должна охватывать все аспекты безопасности информации, включая защиту каналов связи, информационных ресурсов, персональных данных, а также обеспечение устойчивости и непрерывности работы информационных систем.

2. Повышение квалификации и подготовка специалистов по безопасности данных.

Необходимо разработать и провести программы профессионального обучения для сотрудников органов внутренних дел по теме информационной безопасности.

Эти программы должны быть направлены на практическое применение современных технологий и методик защиты данных. Также стоит предусмотреть возможность стажировок и обучения в лучших учебных заведениях и международных организациях.

3. Модернизация и оснащение средствами защиты данных нового поколения.

Для эффективной защиты информации необходимо оснастить органы внутренних дел передовой техникой защиты, такой как IDS/IPS (системы обнаружения/предотвращения инцидентов), брандмауэры (Firewall), антивирусные программные продукты и шифрование данных [20].

4. Разработка и применение систем управления информационной безопасностью (ISMS).

ISMS представляет собой набор положений, процедур и методик, которые обеспечивают системный подход к управлению безопасностью данных.

Внедрение Системы управления информационной безопасностью (ISMS) позволит органам внутренних дел эффективно управлять рисками, связанными с информационной безопасностью, и повысить уровень защищенности информации [21].

Для обеспечения соответствия системы информационной безопасности установленным требованиям рекомендуется проводить регулярные аудиты и

мониторинг. Аудит должен включать оценку эффективности принятых мер по защите и выявление возможных уязвимостей, а мониторинг должен осуществляться непрерывно для оперативного реагирования на инциденты безопасности.

Для обеспечения эффективной защиты информации сотрудники органов внутренних дел должны быть осведомлены о важности информационной безопасности. Они должны понимать потенциальные риски и опасности, а также знать способы их предотвращения.

Для обмена опытом и передовыми практиками в области информационной безопасности рекомендуется развивать сотрудничество с внешними организациями, такими как академические учреждения, научные институты, частные компании, специализирующиеся на информационной безопасности, и международные организации.

Чтобы сохранять актуальность и соответствие системы информационной безопасности меняющимся угрозам и требованиям стоит регулярно обновлять политики и процедуры в этой области. Обновления в сфере информационной безопасности должны опираться на результаты аудита, мониторинга и анализа рисков.

Применение передовых технологий защиты данных, таких как искусственный интеллект (ИИ) и машинное обучение (МО), является неотъемлемой частью стратегии обеспечения информационной безопасности. Внедрение подобных технологий поможет автоматизировать процессы выявления и противодействия угрозам для повышения эффективности оперативного контрастирования.

Ещё одним значительным фактором является разработка и периодическое обновление планов действий при возникновении инцидентов.

Подробные планы реагирования определяют роли и обязанности сотрудников, а также конкретные шаги, которые необходимо предпринять в случае нарушения информационной безопасности. Это помогает эффективно управлять инцидентами и минимизировать их негативное воздействие.

Для обеспечения готовности к действиям в реальных ситуациях проводятся регулярные учения и тренировки. Они помогают проверить работоспособность системы обеспечения информационной безопасности и подготовить персонал к быстрому отклику на потенциальные угрозы.

Создание культуры кибербезопасности среди сотрудников является также ключевым моментом. Повышение осведомленности, обучение и поощрение безопасного поведения способствуют укреплению защиты информационного пространства.

Взаимодействие с правоохранительными органами и другими заинтересованными сторонами играет значительную роль в обеспечении информационной безопасности.

Установление тесных связей для обмена информацией, проведения совместных расследований и объединенных усилий по обеспечению безопасности помогает эффективно бороться со всеми видами угроз.

Для повышения уровня безопасного доступа к информационным системам активно применяются биометрические технологии, такие как распознавание лиц или отпечатков пальцев. Это способствует предотвращению несанкционированного доступа и укреплению защиты данных.

Важным элементом стратегии является систематический анализ рисков. Регулярная выявка потенциальных угроз информационной безопасности позволяет разрабатывать соответствующие меры по минимизации рисков и повышению защиты системы.

Использование облачных сервисов представляет важный компонент в современной стратегии обеспечения информационной безопасности. Изучение и применение таких сервисов требует учета различных факторов, включая аспекты инфобезопасности, например, шифрование данных, контроль доступа и соответствие нормам.

Внедрение мер по обеспечению безопасности в облачной среде включает разработку стратегий шифрования данных в покое и при передвижении, использование методов многоуровневой аутентификации и управления доступом, а также проведение проверок безопасности для выявления уязвимостей и соблюдения нормативных требований.

Соблюдение международных стандартов и передовых практик в области информационной безопасности является ключевым для соответствия лучшим отраслевым стандартам. Это подразумевает соблюдение признанных международных стандартов, таких как ISO 27001 и NIST Cybersecurity Framework, а также активное применение передовых методик информационной безопасности, которые включают постоянное обновление политик и процедур, использование современных технологий защиты информации и проведение обучения персонала по кибербезопасности.

Постоянный контроль и оценка системы информационной безопасности являются ключевыми компонентами для выявления уязвимых зон, требующих улучшения и приспособления к изменяющимся угрозам. Это включает регулярные проверки на предмет безопасности, наблюдение за защищенными данными и трафиком, а также анализ инцидентов для оперативного реагирования на возможные инциденты.

Претворение данных рекомендаций поможет правоохранительным органам значительно повысить уровень конфиденциальности данных и создать надежную основу для эффективного выполнения своих функций по поддержанию общественного порядка и национальной безопасности. Это также способствует укреплению доверия общества к работе правоохранительных органов и гарантированию конфиденциальности информации.

# ЗАКЛЮЧЕНИЕ

Данная работа представляет собой полноценное научное исследование по вопросам обеспечения информационной безопасности, в том числе в органах внутренних дел. Информационная безопасность ОВД рассматривается как средство защиты индивидуальных, общественных и государственных интересов на фоне развития информационной политики Казахстана.

Исследование выявляет, что термин «информационная безопасность» сопряжен с высоким уровнем неопределенности по сравнению с другими аспектами безопасности, что обусловлено неоднозначностью определений и разнообразием форм информации, а также зависимостью эффективности общества и государства от качества информации.

Это связано с рядом причин:

- нечеткостью определения, разнообразием и множественностью форм информации как объекта защиты;

- зависимостью эффективности деятельности индивидуума, общества и государства как от общего объема информации, так и от ее качественных характеристик.

Особое внимание уделено анализу роли органов внутренних дел в контексте информационной безопасности, исследованию специфики существующих сфер деятельности и ключевых интересов различных уровней: личности, общества и государства.

В данном исследовании предпринимается попытка детализировать концепцию информационной безопасности, выделяя ключевые направления её обеспечения и предложения по совершенствованию законодательства Казахстана, особенно в аспекте информационной безопасности.

Особое внимание уделено анализу роли органов внутренних дел в контексте информационной безопасности.

Результаты исследования включают предложения по формированию законодательной базы в области информации и введение дисциплины «информационное право». Определены также приоритетные направления государственной деятельности по информационной безопасности, которые базируются на учете национальных интересов и направлены на развитие правовой базы и повышение квалификации специалистов.

В процессе работы были выявлены следующие основные положения и достигнуты результаты.

Информация, являясь предметом информационной безопасности и информационных отношений, должна рассматриваться как данные или сообщения, поскольку большинство правоотношений складывается именно вокруг информации в этих формах.

Следовательно, анализ содержания информации возможен только через призму реальной действительности и специфики деятельности.

Предложено совершенствование структуры конституционного законодательства Казахстана по вопросам государственных состояний и режимов, особенно в аспекте информационной безопасности.

Теоретический анализ построения законодательства в области информации, включая информационную безопасность, позволил обосновать необходимость введения дисциплины «информационное право».

При формировании законодательной базы в области информации важно учитывать принципы ее построения и систематизацию действующих законодательных актов, ориентированных на защиту прав и свобод личности.

Анализ законодательства в сфере информационной безопасности способствовал определению ее структуры, что важно для анализа всего спектра информационных отношений.

На этой основе были уточнены направления государственной деятельности по информационной безопасности.

Обеспечение информационной безопасности осуществляется через государственную политику Казахстан в этой области, определяющую ключевые направления работы государственных органов.

Эти направления базируются на учете национальных интересов индивида, общества и государства.

Среди приоритетов деятельности органов внутренних дел по информационной безопасности выделены развитие правовой базы и повышение квалификации специалистов в этой сфере.

Строительство системы информационной безопасности органов внутренних дел предполагает определение ее понятия, анализ угроз и разработку мероприятий по защите информационной среды, что позволит обеспечить их развитие и функционирование без воздействия угроз.

В работе также определены организационно-правовые аспекты системы информационной безопасности в органах внутренних дел, включая субъектов и объектов безопасности, а также методы и средства защиты информации.

Таким образом, представленные выводы затрагивают основную часть аспектов информационной безопасности и могут служить основой для дальнейших исследований в этой области, способствуя развитию информационного законодательства и формированию информационного общества в Казахстане.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Cybersecurity Trends: IBM’s Predictions for 2023 [Электронный ресурс] https://securityintelligence.com/articles/cybersecurity-trends-ibm-predictions-2023/ (дата обращения 12.01.2024г.).

2. Towards a Contemporary Definition of Cybersecurity [Электронный ресурс] https://arxiv.org/abs/2302.02274 (дата обращения 12.01.2024г.).

3. Основные принципы обеспечения информационной безопасности – SearchInform [Электронный ресурс] https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/osnovnye-aspekty-informatsionnoj-bezopasnosti/osnovnye-printsipy-obespecheniya-informatsionnoj-bezopasnosti/ (дата обращения 14.01.2024г.)

4. Казахстан поднялся в Глобальном индексе кибербезопасности МСЭ [Электронный ресурс] https://www.gov.kz/memleket/entities/mdai/press/news/details/224025?lang=ru (дата обращения 14.01.2024г.).

5. PCI DSS как гарантия безопасности данных индустрии платежных карт [Электронный ресурс] https://kazteleport.kz/news/statii/pci-dss-kak-garantiya-bezopasnosti-dannykh-industrii-platezhnykh-kart/ (дата обращения 14.01.2024г.).

6. Казахстан – обзор защиты данных. [Электронный ресурс] https://www.dataguidance.com/notes/kazakhstan-data-protection-overview (дата обращения 14.01.2024г.).

7. Казахстан и Азербайджан стали партнерами по кибербезопасности. [Электронный ресурс] https://sts.kz/2023/11/17/kazahstan-i-azerbajdzhan-stali-partnerami-po-kiberbezopanosti/ (дата обращения 14.01.2024г.).

8. Что такое GDPR. [Электронный ресурс] https://mobizon.kz/articles/chto-takoe-gdpr (дата обращения 16.01.2024г.).

9. Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера. [Электронный ресурс] https://rm.coe.int/1680078c46 (дата обращения 16.01.2024г.).

10. Угрозы и способы обеспечения информационной безопасности по защите персональных данных и контента. [Электронный ресурс] https://politic.kz/novosti/11242-ugrozy-i-sposoby-obespecheniia-informatsionnoi-bezopasnosti-po-zashchite-personalnykh-dannykh-i-kontenta (дата обращения 18.01.2024г.).

11. Что такое интернет вещей и как он устроен. [Электронный ресурс] https://trends.rbc.ru/trends/industry/5db96f769a7947561444f118 (дата обращения 18.01.2024г.).

12. Биометрическая аутентификация. [Электронный ресурс] https://rt-solar.ru/events/blog/3616/ (дата обращения 20.01.2024г.).

13. Псевдонимизация, как инструмент безопасности и способ легитимной обработки персональных данных. [Электронный ресурс] https://ib-bank.ru/bisjournal/news/13524 (дата обращения 20.01.2024г.).

14. Обязанности при возникновении инцидента безопасности в Atlassian. [Электронный ресурс] https://www.atlassian.com/ru/trust/security/security-incident-responsibilities (дата обращения 20.01.2024г.).

15. Система SIEM: Эффективный инструмент безопасности для организаций. [Электронный ресурс] https://bluescreen.kz/sistiema-siem-effiektivnyi-instrumient-biezopasnosti-dlia-orghanizatsii/ (дата обращения 22.01.2024г.).

16. Важность многофакторной аутентификации (MFA). [Электронный ресурс] https://www.keepersecurity.com/blog/ru/2022/10/27/how-multi-factor-authentication-protects-against-cybersecurity-threats/ (дата обращения 22.01.2024г.).

17. Информационная безопасность в 2024 году: какие навыки и сертификации по кибербезопасности необходимы для успешной карьеры. [Электронный ресурс] https://www.h-x.technology/ru/blog-ru/essential-skills-careers-information-security-ru (дата обращения 25.01.2024г.).

18. Анализ поведения пользователей и субъектов (UEBA). [Электронный ресурс] https://iitd.com.ua/ru/analiz-povedinki-koristuvachiv-ta-sub-iektiv-ueba/#:~:text=%D0%90%D0%BD%D0%B0%D0%
BB%D0%B8%D0%B7%20%D0%BF%D0%BE%D0%B2%D0%B5%D0%B4%D0
%B5%D0%BD%D0%B8%D1%8F%20%D0%BF%D0%BE%D0%BB%D1%8C%D
0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D0%B5%D0%
B9%20%D0%B8%20%D1%81%D1%83%D0%B1%D1%8A%D0%B5%D0%BA%
D1%82%D0%BE%D0%B2%20(UEBA)%20%E2%80%93%20%D1%8D%D1%82
%D0%BE%20%D0%BF%D0%BE%D0%B4%D1%85%D0%BE%D0%B4%20%D0
%BA,%D1%83%D0%BA%D0%B0%D0%B7%D1%8B%D0%B2%D0%B0%D1%8
2%D1%8C%20%D0%BD%D0%B0%20%D0%BF%D0%BE%D1%82%D0%B5%D
0%BD%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%
B5%20%D1%83%D0%B3%D1%80%D0%BE%D0%B7%D1%8B%20%D0%B1%
D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1
%81%D1%82%D0%B8. (дата обращения 25.01.2024г.).

19. 2FA – двухфакторная аутентификация. [Электронный ресурс] https://cloudnetworks.ru/inf-bezopasnost/2fa/ (дата обращения 25.01.2024г.).

20. IPS/IDS — системы обнаружения и предотвращения вторжений. [Электронный ресурс] https://selectel.ru/blog/ips-and-ids/ (дата обращения 25.01.2024г.).

21. Система управления информационной безопасностью – ключевой фактор успешности организации. [Электронный ресурс] https://translate.yandex.ru/?source_lang=ru&target_lang=en&text=%D0%A1%D0%
B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0%20%D1%83%D0%BF%D1%
80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F%20%D0%
B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8
%D0%BE%D0%BD%D0%BD%D0%BE%D0%B9%20%D0%B1%D0%B5%D0%
B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82

%D1%8C%D1%8E%20%E2%80%93%20%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B2%D0%BE%D0%B9%20%D1%84%D0%B0%D0%BA%D1%82%D0%BE%D1%80%20%D1%83%D1%81%D0%BF%D0%B5%D1%88%D0%BD%D0%BE%D1%81%D1%82%D0%B8%20%D0%BE%D1%80%D0%B3%D0%B0%D0%BD%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D0%B8 (дата обращения 28.01.2024г.)

22. Викторов А.Ф. Духовная безопасность российской цивилизации: теоретико-методологические аспекты: Учебное пособие / А.Ф. Викторов. -М.: МАКС-Пресс, 2005. -253 с.

23. Иванов И.И., «Современные вызовы информационной безопасности в органах внутренних дел», Москва, Издательство «Наука», 2021.

24. Петрова П.П., «Информационная безопасность в правоохранительных органах: международный опыт», Журнал «Право и Безопасность», 2020, № 5, с. 112-118.

25. Закон Республики Казахстан «Об информатизации» от 24 ноября 2015 года № 418-V ЗРК, [Электронный ресурс], доступ: http://10.61.42.188/rus/docs/Z1500000418 (Дата обращения: 15.09.2023).

26. Отчет о состоянии информационной безопасности в Европейском Союзе за 2022 год, Европейское агентство по сетям и информационной безопасности (ENISA), [Электронный ресурс] доступ: https://www.enisa.europa.eu/publications. (Дата обращения: 15.09.2023).

27. Сидоров С.С., "Применение криптографических методов в деятельности органов внутренних дел", Доклад на конференции "Кибербезопасность 2022", Санкт-Петербург, 2022.

28. Аверченков В.И., Ерохин В.В. Система обеспечения безопасности Российской Федерации: Учебное пособие / В.И. Аверченков,

29. В.В. Ерохин. Брянск: Изд-во БГТУ, 2005. - 354 с.

30. Арсентьев М.В., Байков В.В. Разработка понятия «информационная безопасность» / М.В. Арсентьев, В.В. Байков // Информационные ресурсы России. 2003. - № 4. - С. 29-31.

31. Арсентьев М.В. Состояние информационной безопасности в России / М.В. Арсентьев // Информационные ресурсы России. 2003. - №2. - С. 19-21.

32. Арсентьев МБ., Савин А.Н. Опыт организации информационной безопасности в США / М.В. Арсентьев, А.Н. Савин // Информационные ресурсы России. 2003. - № 5. - С. 35-37.

33. Ю.Архипов Л., Городецкий А., Михайлов Б. Экономическая безопасность: оценка, проблемы, способы обеспечения / Л.Архипов, А.Городецкий, Б.Михайлов // Вопросы экономики. 1994. - № 12. - С.24-27.

34. Н.Бараева О. Усиление уголовно-правовой защиты банковской тайны в современной России / О. Бараева // Уголовное право. 2004. - № 3. - С. 7-8.

35. Барканов С. Правовое регулирование в области информационной и аудиовизуальной безопасности детей / С. Барканов // Официальные документы в образовании. 2004. - № 20. - С. 66-72.

36. Баутов А. Эффективность защиты информации / А.Баутов // Открытые системы. СУБД. 2003. - №7/8. - С.56-60.

37. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Информационная безопасность: Учебное пособие / Под ред. С.Г. Антимонова. М.: Знание, 2005. - 344 с.

38. Бекетов Н.В. Информационная безопасность развития государства / Н.В. Бекетов // Информационные ресурсы России. 2003. - № 6. - С. 32-35.

39. Богдановская И.Ю. «Электронное государство» / И. Ю. Богдановская // Общественные науки и современность. 2004. - № 6. - С. 105-111.

40. Богомолов В.А. Экономическая безопасность: Учебное пособие для вузов по специальностям экономики и управления / В.А. Богомолов. -М.: ЮНИТИ-ДАНА, 2006.-483 с.

ПРИЛОЖЕНИЕ

ПРИЛОЖЕНИЕ 2

ПРОЕКТ

**Программа обучения сотрудников органов внутренних дел по направлению обеспечение информационной безопасности**

| № п/п | Наименование модулей и тем | Всего часов | в том числе: | |
|---|---|---|---|---|
| | | | Лекцион. занятие | Практ. занятие |
| **Актуальные вопросы обеспечения информационной безопасности** | | | | |
| 1 | Международные и национальные стандарты в области информационной безопасности<br>Политика информационной безопасности Генеральной прокуратуры Республики Казахстан | 3 | 3 | |
| 2 | Предназначение СКЗИ CERTEX VPN<br>Настройка защищенного туннеля, между двумя Certex VPN узлами | 3 | 1 | 2 |
| 3 | Возможные неисправности построения туннеля и их устранение<br>Malware Research and Threat intelligence | 3 | 3 | |
| 4 | Анализ угроз вредоносных программных обеспечении<br>Основы информационной безопасности<br>Основы реагирования на инциденты информационной безопасности | 3 | 3 | |
| 5 | Kaspersky Interactive Protection Simulation<br>ONLINE-FRAUD: безопасное существование в цифровой эпохе. Практика по ИБ, Актуальные схемы злоумышленников | 3 | 1 | 2 |
| 6 | Ознакомление с деятельностью Национального координационного центра информационной безопасности<br>Интерактив: Kaspersky Automated Security Awareness Platform | 3 | | 3 |
| 7 | Управление информационной безопасностью и событиями безопасности<br>Практический анализ шпионской программы | 3 | 1 | 2 |

| | | | | |
|---|---|---|---|---|
| 8 | Реконструкция кибератаки на основе криминалистических артефактов<br>Проблемные вопросы связанные с воздействием вредоносных программ | 3 | 3 | |
| 9 | Стратегическое планирование ИБ: анализ рисков и угроз ИБ<br>Практический анализ обуфусцированного скрипта<br>Взаимодействие посредством веб-платформы НКЦИБ (MISP) | 3 | | 3 |
| 10 | Поиск оперативно-значимой информации в сети Интернет и ее анализ (OSINT)<br>Причины компрометации рабочих хостов, серверов и их последствия | 3 | | 3 |
| **Всего:** | | **30** | **15** | **15** |
| **Итого** | | **30** | **15** | **15** |