1. Место информационной безопасности в национальной безопасности РФ.

Информационная безопасность занимает ключевое место в системе национальной безопасности Российской Федерации, обеспечивая защиту личности, общества и государства от информационных угроз. В условиях современного глобального информационного пространства национальная безопасность определяется способностью государства сохранять суверенитет, территориальную целостность и устойчивое развитие, что невозможно без надежной защиты информационной инфраструктуры, данных и коммуникаций от кибератак, шпионажа и дезинформации. Информационная безопасность является необходимой основой для обеспечения обороноспособности, предотвращения военных и информационно-психологических воздействий, а также государственной и экономической стабильности.

Стратегия национальной безопасности РФ выделяет информационную безопасность как приоритетное направление, направленное на создание безопасной среды для оборота достоверной информации и устойчивого функционирования критической информационной инфраструктуры. Доктрина информационной безопасности РФ определяет основные задачи по выявлению и противодействию киберугрозам, обеспечению защиты государственных тайн и персональных данных, а также борьбе с пропагандой экстремистских идей и деструктивной информацией. Таким образом, информационная безопасность является неотъемлемой частью системы национальной безопасности, обеспечивая государственный суверенитет и защиту национальных интересов в информационной сфере.

2. Законодательные и правовые основы защиты компьютерной информации и информационных технологий.

Законодательные и правовые основы защиты компьютерной информации и информационных технологий в России базируются на ряде ключевых федеральных законов. Основным законом является Федеральный закон №149-ФЗ «Об информации, информационных технологиях и о защите информации», который определяет основные понятия, виды информации, порядок ее обработки и защиты. Закон вводит требования к конфиденциальной информации, регулирует порядок ограничения доступа к информации и ответственность за ее нарушение. Также важны законы 152-ФЗ «О персональных данных», обеспечивающий защиту личной информации граждан, 98-ФЗ «О коммерческой тайне» и 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», регулирующий защиту информационных систем в стратегически важных отраслях.

Кроме законодательных актов, правовую основу составляют статьи Уголовного кодекса РФ, например, статья 272, которая предусматривает ответственность за неправомерный доступ к компьютерной информации, и другие нормативные акты, указы президента и правительственные постановления, регулирующие информационную безопасность. Эти нормы объединены в систему правовых механизмов, предназначенных для предотвращения киберугроз, защиты информации, обеспечения работоспособности критической инфраструктуры и минимизации рисков, связанных с информационными технологиями.

3. Международные стандарты информационного обмена.

Международные стандарты информационного обмена представляют собой набор согласованных правил, протоколов и процедур, которые обеспечивают совместимость и безопасность обмена данными между разными странами и организациями. Одним из ключевых стандартов в этой области является серия ISO/IEC 27000, разработанная Международной организацией по стандартизации (ISO) и Международной электротехнической комиссией (IEC), которая включает требования по информационной безопасности и защите информации при ее передаче. Важным элементом международного обмена является использование стандартов, таких как XML и HTML, признанных Всемирным консорциумом по веб-стандартам (W3C), обеспечивающих единый формат и структуру данных для их корректного восприятия и обработки в сетях различных стран.

В России международные стандарты информационного обмена регулируются и внедряются с учетом национального законодательства и стандартов (ГОСТ), что позволяет соответствовать мировым требованиям и обеспечивать надежность, безопасность и эффективность передачи информации через государственные и корпоративные границы. Также существуют согласованные документы и соглашения по международному обмену финансовой и иной информацией между странами, что подтверждает активное участие России в глобальном информационном пространстве. Международные стандарты способствуют унификации процессов, повышая доверие к информации и снижая риски искажения данных при трансграничном обмене.

4. ИБ в условиях функционирования в России глобальных сетей.

Информационная безопасность в условиях функционирования в России глобальных сетей становится одной из приоритетных задач из-за высокой уязвимости информационных ресурсов в открытом интернете. Глобальная сеть Интернет, изначально созданная как незащищенная система, не обеспечивает надежного контроля целостности и конфиденциальности информации, что создает угрозу перехвата, искажения или утраты данных. В России проблема осложняется недостаточным развитием законодательной, программной и аппаратной базы защиты информации. Комплексный подход к обеспечению безопасности предусматривает применение физических, организационных и технических мер, таких как идентификация и аутентификация, шифрование, управление доступом, аудит и мониторинг, а также планы реагирования и восстановления после инцидентов.

Кроме того, глобальные сети открывают не только новые возможности, но и предоставляют дополнительные возможности злоумышленникам, что требует постоянного обновления и совершенствования мер защиты. Важным принципом является непрерывность защиты в пространстве и времени, минимизация привилегий и разделение обязанностей. В условиях глобального информационного пространства защитные меры должны учитывать динамичность и сложность современных информационных систем, создавая многоуровневую защиту для уменьшения рисков и обеспечения устойчивости функционирования критически важных инфраструктур. Таким образом, информационная безопасность в России в условиях глобальных сетей требует высокого уровня технологической и организационной подготовки, а также координации на всех уровнях управления.

5. Назначение и задачи в сфере обеспечения ИБ на уровне государства.

Назначение обеспечения информационной безопасности (ИБ) на уровне государства в России заключается в укреплении суверенитета страны в информационном пространстве и создании защищенной среды для безопасности информации и информационной инфраструктуры. Государство ставит цель защитить национальные интересы от угроз информационной безопасности, обеспечить целостность, доступность и конфиденциальность информации, а также поддержать устойчивость функционирования критически важных систем и объектов в разных сферах жизнедеятельности, включая оборону, экономику и социальную сферу. Одновременно важной задачей является защита конституционных прав и свобод граждан при обработке персональных данных и информационных ресурсах.

Основными задачами в сфере ИБ на государственном уровне являются выявление, оценка и предупреждение угроз, разработка и внедрение политики информационной безопасности, нормативно-правового регулирования и координация действий между государственными органами и организациями. Важной задачей также является предотвращение преступлений и противоправных действий, связанных с использованием информационно-коммуникационных технологий, укрепление безопасности критической информационной инфраструктуры, развитие сил и средств информационного противоборства, а также обеспечение приоритетного использования российских информационных технологий. Государство также способствует международному сотрудничеству в области ИБ, чтобы установить международно-правовые механизмы защиты информации и предотвращения киберугроз.

6. BS 25999 и ГОСТ Р 53647 – управление непрерывностью бизнеса.

Стандарт BS 25999 — это британский стандарт по управлению непрерывностью бизнеса (BCM), который стал одной из основ для международного стандарта ISO 22301. Он включает две части: первая — рекомендации и практическое руководство по управлению непрерывностью бизнеса; вторая — требования к системе управления непрерывностью, основанные на цикле Деминга PDCA (Планируй–Выполняй–Проверяй–Действуй). BS 25999 помогает организациям идентифицировать потенциальные угрозы, оценить их влияние на бизнес-процессы и разработать стратегии по обеспечению способности быстро восстанавливаться после инцидентов, сохраняя интересы заинтересованных сторон и защищая репутацию компании.

ГОСТ Р 53647 — российский национальный стандарт, адаптированный с учетом BS 25999. Он содержит руководящие указания и требования к менеджменту непрерывности бизнеса, также основан на цикле PDCA, и включает процессы планирования, внедрения, мониторинга и улучшения системы управления непрерывностью. ГОСТ Р 53647 ориентирован на российские реалии и может применяться организациями всех форм собственности для повышения устойчивости бизнеса к рискам и инцидентам. В отличие от BS 25999, внедрение ГОСТ Р 53647 не является обязательным на законодательном уровне в России, однако способствует закреплению эффективных практик управления непрерывностью и улучшению деловой репутации.

7. СТО БР ИББС-1.0 – общие положения в области обеспечения ИБ организаций банковской системы Российской Федерации.

Стандарт Банка России СТО БР ИББС-1.0 «Общие положения» устанавливает базовые требования и рекомендации по обеспечению информационной безопасности организаций банковской системы Российской Федерации. Его основная цель — повышение доверия к банковской системе и обеспечение стабильности функционирования банков и всей платежной системы России. Стандарт направлен на установление единых требований по защите информационных активов банков, предотвращению и снижению ущерба от инцидентов информационной безопасности, а также повышение эффективности мер по обеспечению и поддержанию информационной безопасности.

Документ распространяется на все организации банковской системы РФ, включая Банк России, кредитные организации и представительства иностранных банков. Он рекомендован для добровольного применения и призван гармонизировать подходы к информационной безопасности в банковском секторе, учитывая специфику технологических процессов и автоматизированных банковских систем. Внедрение стандарта способствует снижению рисков сбоев и инцидентов, которые могут привести к серьезным последствиям для всей системы платежей и финансовой стабильности государства.

8. СТО БР ИББС-1.1 – аудит ИБ 78.

Стандарт Банка России СТО БР ИББС-1.1-2007 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности» регламентирует требования и методологию проведения аудита ИБ в организациях банковской системы РФ. Аудит ИБ рассматривается как ключевой процесс в цикле менеджмента информационной безопасности, направленный на оценку соответствия уровня защиты информации требованиям стандарта СТО БР ИББС-1.0. Он способствует повышению доверия к организациям банковской системы и позволяет выявлять уязвимости, ошибки и пробелы в решениях и мерах по обеспечению ИБ.

Стандарт включает этапы подготовки к аудиту, анализа документов, проведения проверки на местах, а также составления и согласования отчета по результатам аудита. Документ распространяется не только на банки, но и на организации, участвующие в проведении аудита ИБ банковских структур. Он рекомендован для применения и лежит в основе разработки программ аудита ИБ и нормативных актов в банковской сфере. Содержание стандарта ориентировано на обеспечение комплексной и системной оценки уровня информационной безопасности с учетом отраслевых особенностей банковской системы России.

9. СТО БР ИББС-1.2 – методика оценки соответствия ИБ организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0.

Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям стандарта Банка России СТО БР ИББС-1.0 изложена в СТО БР ИББС-1.2. Основная цель методики — стандартизация подходов и способов оценки уровня соответствия обеспечения информационной безопасности в банковских организациях установленным требованиям. Оценка проводится по трём направлениям: текущий уровень информационной безопасности организации, менеджмент информационной безопасности и уровень осознания значимости информационной безопасности в организации.

Методика предусматривает использование групповых и частных показателей, которые оцениваются экспертами на основе установленной шкалы: «нет» (0), «частично» (0,25, 0,5 или 0,75) и «да» (1). Частные показатели делятся на обязательные и рекомендательные, что влияет на способы их оценивания. Итоговый уровень соответствия формируется на основе совокупности оценок по всем показателям и служит основой для принятия управленческих решений по совершенствованию системы информационной безопасности в организации банковской системы РФ. Методика применяется как при внутреннем самоаудите, так и при внешних проверках.

10. Рекомендации по стандартизации Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации. (утв. Приказом Ростехрегулирования от 06.04.2005 № 77-ст).

Рекомендации по стандартизации Р 50.1.053-2005 «Информационные технологии. Основные термины и определения в области технической защиты информации» утверждены Приказом Ростехрегулирования от 06.04.2005 № 77-ст и введены в действие с 1 января 2006 года. Этот документ устанавливает ключевые термины и определения, которые используются в сфере технической защиты информации при применении информационных технологий. Цель рекомендаций — стандартизировать язык и понятия для единого понимания процессов и средств защиты информации от несанкционированного доступа, утечки, искажения и других угроз.

В стандарте определены такие понятия, как защищаемая информация, безопасность информации, перехват информации, доступ в автоматизированной информационной системе, техническая защита информации, а также субъекты доступа и объекты защиты. Данные рекомендации применяются во всех видах технической документации и научно-технической литературе по защите информации. Документ служит фундаментом для разработки конкретных мер и систем защиты информации, обеспечивая единообразие и согласованность терминологии в области информационной безопасности и технической защиты информации.

11. Рекомендации по стандартизации Р 50.1.056-2005. Техническая защита информации. Основные термины и определения. (утв. Приказом Ростехрегулирования от 29.12.2005 № 479-ст).

Рекомендации по стандартизации Р 50.1.056-2005 «Техническая защита информации. Основные термины и определения» утверждены Приказом Ростехрегулирования от 29.12.2005 № 479-ст и введены в действие с 01.06.2006. Этот документ устанавливает систематизированный перечень терминов и определений, используемых в области технической защиты информации в различных сферах деятельности. Цель стандарта — обеспечение единообразия и точности понятийного аппарата для эффективной коммуникации и разработки технических мер по защите информации от несанкционированного доступа, утечек и иных угроз.

В стандарте определены основные понятия, связанные с безопасностью информации, объектами и средствами технической защиты, уязвимостями, угрозами и субъектами доступа. Документ охватывает такие термины, как техническая защита информации, безопасность информации, технические средства защиты от утечек по техническим каналам, информационные технологии и другие ключевые концепции. Рекомендации применяются в нормативных актах, технической документации и научно-технической литературе, служат основой для разработки систем технической защиты информации и реализации эффективных мер информационной безопасности.