УДК:34.002

ПРАВОВЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Шоокумова Д.П.,, к.ю.н., доцент
Ошский государственный университет
dshookumova@mail.ru
Ош, Кыргызстан
Ибраимов Б.З., ст.преподаватель
Ошский государственный университет
Ош, Кыргызстан

Аннотация:*Подробно раскрываются основные институты информационного права: информационной безопасности, персональных данных, электронного документооборота, правового регулирования СМИ и др. Особое внимание в работе уделено механизмам борьбы с информационное преступностью и обеспечения информационное безопасности.*

Ключевые слова: *информация, институт, основа, персонал, право,механизм,документ*

УКУКТУК НЕГИЗДЕРИ МААЛЫМАТТЫК КООПСУЗДУКТУ КАМСЫЗ КЫЛУУ

Шокумова П.Д., ю.и. к., доцент
Ош мамлекеттик университети
dshookumova@mail.ru
Ош, Кыргызстан
Ибраимов Б.З., ага окутуучу
Ош мамлекеттик университети
Ош, Кыргызстан

Аннотация: *Маалыматтык укуктун негизги институттары деталдуу түрдө ачылган: маалыматтык коопсуздук, жеке маалыматтар, электрондук документ жүгүртүү, ЖМКны укуктук жөнгө салуу жана башкалар. Маалыматтык кылмыштуулук менен күрөшүү жана маалыматтык коопсуздукту камсыздоо механизмдерине өзгөчө көңүл бурулат.*

Ачкыч сөздөр: *маалымат, институт, негиз, персонал, укук, механизм, документ*

LEGAL BASIS FOR ENSURING INFORMATION SECURITY

D.P.Shookumova Candidate of Law, Associate Professor
Osh State University,
Osh, Kyrgyzstan
D.P.Shookumova B. Z.Ibraimov Senior Lecturer
Osh State University
Osh, Kyrgyzstan

Abstract: *The main institutions of information law are disclosed in detail: information security, personal data, electronic document management, legal regulation of the media, etc. Particular attention is paid to the mechanisms of combating information crime and ensuring information security.*

Keywords: *information, institute, foundation, personnel, law, mechanism,document.*

Основные проблемы национальной безопасности Кыргызстана на современном этапе состояние национальной безопасности Кыргызской Республики в большей степени определяется внутриполитическими процессами в стране. Оно характеризуется не принципиальным нарушением ранее сложившихся (в период с 19932005 гг.) отношений и связей: между Президентом, исполнительной, законодательной, судебной ветвями власти и гражданского общества.

При этом, приход нового высшего руководства в управление страной, граждане Кыргызстана связывают с надеждами на позитивные изменения в жизни: как личной, так и всего общества и государства в целом. Действующим властям население оказывает кредит доверия, который, в свою очередь, может быть исчерпан, если будут отсутствовать какие-либо конкретные шаги со стороны властей на существенное улучшение уровня жизни, прежде всего, для социально уязвимых слоев общества. Обществу также необходимы определенные реформы, практические результаты от которых, будут видны уже в обозримом будущем. В противном случае Кыргызстан может столкнуться с вновь набирающим силу разрывом между обществом и властью, что приведет к дестабилизации внутриполитической обстановки.

Быстроизменяющаяся внутренняя обстановка в 2005 году охарактеризовалась жесткой борьбой различных политических сил и интересов на парламентских выборах, сменой власти и проведением президентских выборов. Результаты этих событий непосредственным образом зависели от «народного» фактора. Мартовские события показали, к каким кардинальным изменениям для республики может привести массовое недовольство населения действиями руководства страны и органов власти. Анализ причин, хода и последствий массовых протестных акций в 2005 году свидетельствует об усилении роли гражданского общества во взаимоотношениях с государственными институтами власти и управления, об отсутствии единства и ответственности в системе исполнительной власти, отсутствии должного взаимодействия центральных и местных органов власти, как между собой, так и с населением, что в конечном счете не повышает и не обеспечивает общественно-политическую стабильность.

С другой стороны, имевшие место в 2005 году политические события показали, насколько наши граждане, в отсутствии «общей национальной идеи», подвержены влиянию определенных политических сил и готовы поддержать экстремистские идеи отдельных лиц и организаций. Также, эти события выявили неготовность правоохранительных и других государственных органов к предотвращению и локализации конфликтных и кризисных ситуаций.

В республике присутствуют факторы, способствующие усилению религиозного экстремизма и национализма. Это особый спектр угроз. Попытки пропаганды религиозного экстремизма имеют место не только в южных, но и в северных регионах страны, несмотря на активные действия правоохранительных органов и спецслужб по нейтрализации деятельности активных членов и распространителей идей «Хизбут-Тахрир». При этом действия экстремистов приобретают все более четко выраженную политическую направленность. Одним из их требований является отмена в республике русского языка, как официального, что очень схоже и соответствует планам западных политиков, которые стремятся вытеснить Россию из этого региона, стараясь провести через отдельных коррумпированных политиков раскол в обществе, ратуя за ведение делопроизводства исключительно на кыргызском языке, забывая при этом, что это только увеличит отток русскоязычного населения из страны, среди которых отличные специалисты в различных областях.

Зачем уподобляться странам, ограничивая себя? Во все времена приветствовалось и являлось показателем образованности человека — знание языков. Многоязычие никому не мешает и не ущемляет, и не принижает значимость государственного языка, а наоборот

расширяет кругозор любого человека. И в этом деликатном вопросе нужна не какая-то крайняя мера, а грамотная политика по обучению населения государственному и официальному языкам. Здесь можно сделать сравнение с такой страной, как Швейцария — единственная страна в Европе, где сразу четыре национальных языка имеют статус официального государственного: немецкий, французский, итальянский и реторомanский. В этом случае никому не приходит в голову отменить один из них, несмотря на то, что 74% граждан этой страны родным считают немецкий язык.

В нашем случае, русский язык является языком межнационального общения не только внутри нашей многонациональной республики, но и на всем пространстве СНГ, что способствует экономическому, культурному

развитию нашей республики и, что очень не нравится отдельным заокеанским политикам. Им будет выгодно, если нас не будет больше объединять наша общая богатая история и русский язык. Это, как в сказке про братьев, которых нельзя победить, когда они вместе и, легко, когда они поодиночке.

Стали фиксироваться проявления национализма. Часть узбекской диаспоры юга выступила с требованиями о придании официального статуса этническому языку и увеличении числа узбеков в структурах власти. Обострению межнациональных отношений способствует неурегулированность пограничных вопросов с Республикой Узбекистан и Республикой Таджикистан на юге страны. В частности, в Джалал-Абадской области имеется около 80 спорных участков. 2025 процентов населения, проживающего в районах их расположения, составляют узбеки и таджики. В Ошской области насчитывается 15 водоземельных спорных участков. Все это делает возможным искусственное разжигание бытовых межэтнических конфликтов, особенно в местах компактного проживания национальных диаспор.

Росту религиозного экстремизма и национализма способствует деятельность в республике иностранных нетрадиционных конфессий, которые насаждают в молодежной среде чуждые, и, по существу антипатриотические ценности. Большинство коренного населения недовольно этим, в связи с чем отмечаются случаи возникновения конфликтных ситуаций на межконфессиональной основе.

Несмотря на значительные потери, понесенные международными террористическими организациями «Аль-Каида», «Движение Талибан» и ИДУ в ходе проведения антитеррористической операции в ИГА, они окончательно не разгромлены. Их главари ушли в подполье и в этих условиях ведут перегруппировку своих разрозненных сил для развертывания диверсионно-террористической деятельности.

Следует ожидать, что нелегальная подпольная деятельность сторонников религиозных экстремистов на территории стран Центральной Азии, в том числе Кыргызстана, активизируется: их основные усилия будут направлены на вербовку в свои ряды молодежи, лиц из среды организованной преступности, подкуп и привлечение на свою сторону сотрудников правоохранительных органов, коррумпированных госчиновников. Через них террористы, вероятно, попытаются разжигать межнациональные, межрелигиозные и водоземельные конфликты, в этих целях проводить теракты и диверсии.

Есть основания полагать, что активизировалась деятельность иностранных спецслужб и используемых ими организаций на территории нашей республики.

Актуальной остается проблема уйгурского сепаратизма в Китае, имеющая тенденцию к обострению обстановки на территории Кыргызской Республики. Уйгурские сепаратисты, так же как боевики ИДУ, тесно интегрировались с международными террористическими центрами и спонсорами, приобрели значительный военный и диверсионный опыт работы в условиях глубокого подполья. Так, например, международные террористические организации уйгурских сепаратистов «Шат» и «Штип» в 1998-2002 гг. совершили ряд дерзких терактов на территории КР. Распространение наркотиков в Кыргызстане продолжает существенно влиять на национальную безопасность. Потребление наркотических веществ растет, что создает угрозу здоровью нации. В стране на диспансерном учете состоит свыше 5 тысяч наркоманов. Однако, по данным ООН, в республике насчитывается от 80 до 100 тысяч наркозависимых людей. Отмечены факты потребления наркотиков с 10-12-летнего возраста. В связи с этим острую проблему стала представлять подростковая наркомания, т.к. ей сопутствует рост детской проституции и бродяжничества.

Перемещение центра мирового производства наркотиков в Афганистан, последовавший за этим рост их транзита через страны Центральной Азии в страны СНГ и Западной Европы, содействовали резкому снижению цен на рынке незаконного оборота наркотиков в регионе и, в частности, Кыргызстане. Транзит наркотиков через территорию Кыргызстана оценивается примерно в 30-35 тонн в год.

Кроме этого, в Кыргызстане имеется собственная значительная сырьевая база в виде зарослей дикорастущей конопли и эфедры, сохраняется практика культивации опийного мака. Среднегодовая стоимость изымаемых в Кыргызстане наркотиков оценивается в 2,5-3 млн. долларов США. По некоторым оценкам, правоохранительные органы изымают не более 10 процентов от общего объема контрабанды наркотиков. Использование даже малой части этих средств, для финансирования международного терроризма и организованной преступности усилит нестабильность в республике и регионе в целом.

Недостаточное осуществление и реализация реформ в экономической, военной, правоохранительной, социальной сферах государственной деятельности, ослабление системы государственного регулирования и

контроля, несовершенство правовой базы, снижение духовно-нравственного потенциала общества — все это в совокупности являются основными факторами, способствующими росту преступности, особенно ее организованных форм, а также коррупции.

В условиях повышения активности разнородных политических и общественных сил, а также местных общин, незаконные или неадекватные действия властных структур вызывают резкую реакцию населения, что может привести к дестабилизации обстановки в отдельно взятом регионе и, в целом, в стране. Люди присоединяются или поддерживают те или иные партии и организации, а также их лидеров и идеи, в основном протестуя против низкого уровня жизни, противоправных действий или бездействия местных органов власти. В результате, значительная часть населения, в том числе безработная молодежь, становиться реальной опорой деструктивных сил. Особую остроту приобретает угроза криминализации общественных отношений, складывающихся в процессе реформирования социально-политического устройства и экономической деятельности.

При этом ситуацией, возникающей в результате некомпетентных управленческих действий или бездействия правительственных органов, активно пользуются не только радикальная политическая оппозиция, но и религиозные экстремистские организации, сепаратистские и иные деструктивные силы.

Обстановка по обеспечению экономической безопасности страны остается сложной и неоднозначной. Масштабы экономических преступлений, а также низкая финансовая дисциплина оказывают отрицательное влияние на исполнении доходной части государственного бюджета. Экономические преступления наносят ощутимый ущерб экономике республики, порождают очаги социальной напряженности и создают условия для дестабилизации общественно-политической обстановки в стране.

Наиболее пораженными коррупцией оказались структуры государственной власти и управления. Широкое распространение коррупция получила и в таких сферах народного хозяйства, как добыча, переработка сырья, торговля, выпуск и перевозка промышленной продукции и продовольственных товаров, строительство. Особенно негативное влияние данное явление оказывает на процесс разгосударствления и приватизации государственной и муниципальной собственности.

Ощутимый ущерб интересам государства и общества наносят хищение материальных ценностей, нецелевое использование бюджетных и кредитных

средств, злоупотребления должностным положением. Ответственные за реализацию инвестиционных проектов министерства и ведомства крайне неэффективно осуществляют работу в данном направлении, в особенности на стадии подготовки проектов. При использовании международных кредитов и финансовой помощи необоснованно высокими являются расходы на оплату услуг иностранных специалистов, закупку оргтехники и офисного оборудования. Во многих случаях инициатива отдается иностранцам, и дальнейшая реализация проекта осуществляется под их диктовку без учета интересов республики. Ущерб экономике наносит контрабанда. К основным методам незаконного импорта-экспорта товаров относятся использование подложных документов, обход таможенных постов, сокрытие от таможенного досмотра, ввоз товаров под видом транзита с последующей его реализацией внутри страны.

Одной из серьезных угроз является — ухудшение экологической ситуации в стране и истощение ее природных ресурсов, что находится в прямой зависимости от состояния экономики и готовности общества осознать глобальность и важность этой проблемы.

Серьезную опасность представляют собой места захоронения радиоактивных отходов. В связи с недостатком финансовых и материальных средств на их содержание и профилактику, они в перспективе под воздействием природных и техногенных катаклизм могут стать источником экологической катастрофы не только для Кыргызстана, но всего региона Центральной Азии. На территории республики находятся 23 хранилища отходов уранового производства, общее число объектов хранения отходов горнорудной промышленности составляет более 130. Оценочно, в случае выбросов урановых отходов на юге КР в зоне бедствия окажутся районы Ферганской долины, относящиеся к Кыргызстану, Узбекистану, Таджикистану, а также Казахстана. Пагубному воздействию от зараженной воды и земли могут быть подвержены более 4 млн. жителей указанных районов. Для решения данной проблемы, по моему мнению, необходимо внедрить уже имеющиеся на вооружении других стран новейшие научные разработки и технологии для контроля затакого рода объектами, а также строго соблюдать научно обоснованные нормативы природопользования и охраны окружающей природной среды. Особое внимание необходимо обратить на недопущение не контролированного ввоза экологически опасных технологий, веществ, материалов. На данный момент состояние внешней безопасности, как составной части национальной безопасности, республики

продолжает характеризоваться низким уровнем угрозы военной агрессии или широкомасштабного вооруженного конфликта, следствием которых могла бы стать утрата республикой суверенитета. Кыргызстан находится сейчас в достаточно сильном международном договорно-правовом поле, фактически исключающем вооруженное нападение на нас сопредельных государств или мировых держав и коалиций (США, Россия, Китай, НАТО). С одной стороны, Договор о коллективной безопасности стран СНГ, а с другой, — участие в Шанхайской организации сотрудничества и активное содействие проведению антитеррористической кампании являются гарантией ненападения. В условиях сохранения Кыргызской Республикой нынешнего внешнеполитического курса на развитие и углубление межгосударственных отношений, прежде всего с ведущими странами мира, усиление для республики внешней военной опасности в среднесрочной перспективе представляется маловероятным.

В экономической сфере уровень внешней угрозы национальной безопасности Кыргызстана определяется в основном характером и степенью негативного воздействия других государств на экономику республики. Ее определенная зависимость от экономик других республик СНГ, нехватка государственных средств на инвестирование крупных проектов, невысокая

конкурентоспособность национальной промышленной продукции, отток капитала за рубеж, неразвитость коммерческого сектора в сфере производства, пограничные барьеры и таможни, а также другие обстоятельства делают экономику КР сильно уязвимой от вмешательства извне. Республика имеет чрезвычайно выгодное геостратегическое положение в регионе Центральной Азии. В ней имеется огромное количество жизненно важных водных ресурсов, большой потенциал для развития электроэнергетики и сельскохозяйственной промышленности. Данные факторы вызывают у сильных в экономическом отношении стран и международных финансовых организаций «соблазн» установить контроль в ущерб сбалансированному экономическому развитию Кыргызстана за теми отраслями экономики, которые могут развиваться на собственной ресурсной базе КР.

В последние годы просматривается тенденция к усилению информационного давления на республику, организованному рядом отечественных и зарубежных СМИ, оппозиционных партий и движений, правозащитных организаций, политических кругов некоторых государств, в том числе и США. Оно осуществляется по известному в прошлом сценарию с обвинением в массовых нарушениях прав человека, ущемлении деятельности

независимых СМИ в Кыргызстане, его отходе от демократии к авторитаризму. Оказываемое на республику информационное давление сопровождается моральной и материальной поддержкой США через международные неправительственные организации блоку непримиримой оппозиции, ряду НПО и нечистоплотных СМИ в КР. США начали активно продвигать отработанные в других странах информационные технологии и методы воздействия, направленные на консолидацию оппозиционных сил и независимых СМИ КР в целях расширения их возможностей по использованию информационных ресурсов и рынка информационных услуг для идеологического и иного воздействия на общественное мнение в республике и за ее пределами, тем самым расшатывая хрупкую внутриэкономическую и политическую структуру республики, а также ее единство. Для недопущения таких тенденций необходимо принятие комплексных мер по защите своего информационного пространства, выявление и устранение причин информационной дискриминации, внедрение необходимых средств и режимов получения, распространения и использования общественно-значимой информации, а также устранение негативных факторов информационной экспансии со стороны других государств.

Исходя из выше изложенного, основным источником внутренней и внешней угрозы национальной безопасности Кыргызской Республики на данный момент и ближнесрочную перспективу следует считать внутриполитическую нестабильность. Нейтрализация этой угрозы требует разработки и реализации комплекса мер, относящихся к компетенции различных структур законодательной и исполнительной власти. Целью этих мер должно стать обеспечение условий для продолжения демократического и безопасного развития страны в правовом поле. Однако без непрерывной координации усилий всех государственных органов достижение этой цели может быть затруднено. Такую координацию могла бы, на наш взгляд, обеспечить межведомственная комиссия по общественной безопасности, которую целесообразно создать при Совете Безопасности КР.

В настоящее время требуется усилить роль государства в экономическом и духовном возрождении Кыргызстана, создании условий для развития гражданского общества, определения полномочий и ответственности общественных и государственных институтов. Властным структурам необходимо добиться доверия общества, а обществу доверить действующим властям управление государством. В связи с развитием информационных

технологий и компьютеризацией экономики одним из важнейших вопросов в деятельности компании становится обеспечение информационной безопасности.Информация – это один из самых ценных и важных активов любого предприятия и должна быть надлежащим образом защищена.

Информационная безопасность – это сохранение и защита информации, а также ее важнейших элементов, в том числе системы и оборудование, предназначенные для использования, сбережения и передачи этой информации. Другими словами, это набор технологий, стандартов и методов управления, которые необходимы для защиты информационной безопасности.

Цель обеспечения информационной безопасности – защитить информационные данные и поддерживающую инфраструктуру от случайного или преднамеренного вмешательства, что может стать причиной потери данных или их несанкционированного изменения. Информационная безопасность помогает обеспечить непрерывность бизнеса.

Для успешного внедрения систем информационной безопасности на предприятии необходимо придерживаться трех главных принципов:

1. **Конфиденциальность.** Это значит ввести в действие контроль, чтобы гарантировать достаточный уровень безопасности с данными предприятия, активами и информацией на разных этапах деловых операций для предотвращения нежелательного или несанкционированного раскрытия. Конфиденциальность должна поддерживаться при сохранении информации, а также при транзите через рядовые организации независимо от ее формата.

2. **Целостность.** Целостность имеет дело с элементами управления, которые связаны с обеспечением того, чтобы корпоративная информация была внутренне и внешне последовательной. Целостность также гарантирует предотвращение искажения информации.

3. **Доступность.** Доступность обеспечивает надежный и эффективный доступ к информации уполномоченных лиц. Сетевая среда должна вести себя предсказуемым образом с целью получить доступ к информации и данным, когда это необходимо. Восстановление системы по причине сбоя является важным фактором, когда речь идет о доступности информации, и такое восстановление также должно быть обеспечено таким образом, чтобы это не влияло

Нужно понимать, что лишь системный и комплексный подход к защите может обеспечить информационную безопасность. В системе

информационной безопасности нужно учитывать все актуальные и вероятные угрозы и уязвимости. Для этого необходим непрерывный контроль в реальном времени. Контроль должен производиться 24/7 и охватывать весь жизненный цикл информации – от момента, когда она поступает в организацию, и до ее уничтожения или потери актуальности.

Выбор и внедрение подходящих видов контроля безопасности поможет организации снизить риск до приемлемых уровней. Выделяют следующие виды контроля:

- **Административный.** Административный вид контроля состоит из утвержденных процедур, стандартов и принципов. Он формирует рамки для ведения бизнеса и управления людьми. Законы и нормативные акты, созданные государственными органами, также являются одним из видов административного контроля. Другие примеры административного контроля включают политику корпоративной безопасности, паролей, найма и дисциплинарные меры.

- **Логический.** Логические средства управления (еще называемые техническими средствами контроля) базируются на защите доступа к информационным системам, программном обеспечении, паролях, брандмауэрах, информации для мониторинга и контроле доступа к системам информации.

- **Физический.** Это контроль среды рабочего места и вычислительных средств (отопление и кондиционирование воздуха, дымовые и пожарные сигнализации, противопожарные системы, камеры, баррикады, ограждения, замки, двери и др.).

Угрозы информационной безопасности можно разделить на следующие:

- **Естественные** (катаклизмы, независящие от человека: пожары, ураганы, наводнение, удары молнии и т.д.).

- **Искусственные,** которые также делятся на:

- непреднамеренные (совершаются людьми по неосторожности или незнанию);
- преднамеренные (хакерские атаки, противоправные действия конкурентов, месть сотрудников и пр.).

- **Внутренние** (источники угрозы, которые находятся внутри системы).
- **Внешние** (источники угроз за пределами системы)

Так как угрозы могут по-разному воздействовать на информационную систему, их делят на пассивные (те, которые не изменяют структуру и содержание информации) и активные (те, которые меняют структуру и содержание системы, например, применение специальных программ).

Наиболее опасны преднамеренные угрозы, которые все чаще пополняются новыми разновидностями, что связано, в первую очередь, с компьютеризацией экономики и распространением электронных транзакций. Злоумышленники не стоят на месте, а ищут новые пути получить конфиденциальные данные и нанести потери компании.

Чтобы обезопасить компанию от потери денежных средств и интеллектуальной собственности, необходимо уделять больше внимания информационной безопасности. Это возможно благодаря средствам защиты информации в лице передовых технологий.

Средства защиты информационной безопасности.Средства защиты информационной безопасности — это набор технических приспособлений, устройств, приборов различного характера, которые препятствуют утечке информации и выполняют функцию ее защиты.Средства защиты информации делятся на:

- **Организационные.** Это совокупность организационно-технических (обеспечение компьютерными помещениями, настройка кабельной системы и др.) и организационно-правовых (законодательная база, статут конкретной организации) средств.
- **Программные.** Те программы, которые помогают контролировать, хранить и защищать информацию и доступ к ней.
- **Технические (аппаратные).** Это технические виды устройств, которые защищают информацию от проникновения и утечки.
- **Смешанные аппаратно-программные.** Выполняют функции как аппаратных, так и программных средств.

В связи со стремительным развитием ИТ, все более частыми кибератаками, компьютерными вирусами и другими появляющимися угрозами наиболее распространенными и востребованными на сегодняшний день являются программные средства защиты информации.

Виды средств защиты информации :Антивирусные программы — программы, которые борятся с компьютерными вирусами и возобновляют

зараженные файлы. Облачный антивирус (CloudAV) – одно из облачных решений информационной безопасности, что применяет легкое программное обеспечение агента на защищенном компьютере, выгружая большую часть анализа информации в инфраструктуру провайдера. CloudAV – это также решение для эффективного сканирования вирусов на приспособлениях с невысокой вычислительной мощностью для выполнения самих сканирований. Некоторые образцы облачных антивирусных программ – это Panda Cloud Antivirus, Crowdstrike, Cb Defense и Immunet.

DLP (Data Leak Prevention) решения – это защита от утечки информации. Предотвращение утечки данных (DLP) представляет собой набор технологий, направленных на предотвращение потери конфиденциальной информации, которая происходит на предприятиях по всему миру. Успешная реализация этой технологии требует значительной подготовки и тщательного технического обслуживания. Предприятия, желающие интегрировать и внедрять DLP, должны быть готовы к значительным усилиям, которые, если они будут выполнены правильно, могут значительно снизить риск для организации. Криптографические системы – преобразование информации таким образом, что ее расшифровка становится возможной только с помощью определенных кодов или шифров (DES – Data Encryption Standard, AES – Advanced Encryption Standard). Криптография обеспечивает защиту информации и другими полезными приложениями, включая улучшенные методы проверки подлинности, дайджесты сообщений, цифровые подписи и зашифрованные сетевые коммуникации. Старые, менее безопасные приложения, например Telnet и протокол передачи файлов (FTP), медленно заменяются более безопасными приложениями, такими как Secure Shell (SSH), которые используют зашифрованные сетевые коммуникации. Беспроводная связь может быть зашифрована с использованием таких протоколов, как WPA/WPA2 или более старый (и менее безопасный) WEP. Проводные коммуникации (такие как ITU-T G.hn) защищены с использованием AES для шифрования и X.1035 для аутентификации и обмена ключами. Программные приложения, такие как GnuPG или PGP, могут применяться для шифрования информационных файлов и электронной почты.Межсетевые экраны (брандмауэры или файрволы) – устройства контроля доступа в сеть, предназначенные для блокировки и фильтрации сетевого трафика. Брандмауэры обычно классифицируются как сетевые или хост-серверы. Сетевые брандмауэры на базе сети расположены на шлюзовых компьютерах LAN, WAN и интрасетях. Это либо программные устройства,

работающие на аппаратных средствах общего назначения, либо аппаратные компьютерные устройства брандмауэра. Брандмауэры предлагают и другие функции для внутренней сети, которую они защищают, например, являются сервером DHCP или VPN для этой сети. Одним из лучших решений как для малых, так и для больших предприятий являются межсетевые экраны CheckPoint. VPN (Virtual Private Network). Виртуальная частная сеть (VPN) дает возможность определить и использовать для передачи и получения информации частную сеть в рамках общедоступной сети. Таким образом, приложения, работающие по VPN, являются надежно защищенными. VPN дает возможность подключиться к внутренней сети на расстоянии. С помощью VPN можно создать общую сеть для территориально отдаленных друг от друга предприятий. Что касается отдельных пользователей сети – они также имеют свои преимущества использования VPN, так как могут защищать собственные действия с помощью VPN, а также избегать территориальные ограничения и использовать прокси-серверы, чтобы скрыть свое местоположение. Proxy-server (Прокси-сервер) – это определенный компьютер или компьютерная программа, которая является связывающим звеном между двумя устройствам, например, такими как компьютер и другой сервер. Прокси-сервер можно установить на одном компьютере вместе с сервером брандмауэра, или же на другом сервере. Плюсы прокси-сервера в том, что его кэш может служить для всех пользователей. Интернет-сайты, которые являются наиболее часто запрашиваемыми, чаще всего находятся в кэше прокси, что несомненно удобно для пользователя. Фиксирование своих взаимодействий прокси-сервером служит полезной функцией для исправления неполадок. Системы мониторинга и управления информационной безопасностью, SIEM. Чтобы выявлять и реагировать на возникающие угрозы информационной безопасности, используется решение SIEM, которое выполняет сбор и анализ событий из разных источников, таких как межсетевые экраны, антивирусы, IPS, оперативные системы и т.п. Благодаря системе SIEM у компаний появляется возможность централизованно хранить журналы событий и коррелировать их, определяя отклонения, потенциальные угрозы, сбои в работе ИТ-инфраструктуры, кибератаки и т.д. Отдельное внимание стоит уделять управлению мобильными устройствами на предприятии, так как многие сотрудники часто используют личные смартфоны, планшеты и ноутбуки в корпоративных целях. Внедрение специальных решений, таких как VMware AirWatch, IBM MaaS360, Blackberry Enterprise Mobility Suite, VMware Workspace One помогут лучше

контролировать мобильные устройства сотрудников и защитить данные компании. ***Заключение:***Информация очень важна для успешного развития бизнеса, следовательно, нуждается в соответствующей защите. Особенно актуально это стало в бизнес-среде, где на передний план вышли информационные технологии. Так как мы живем в эпоху цифровой экономики, без них рост компании просто невозможен. Информация сейчас подвергается все большему числу угроз и уязвимостей. Хакерские атаки, перехват данных по сети, воздействие вирусного ПО и прочие угрозы приобретают более изощренный характер и набирают огромный темп. Отсюда возникает необходимость внедрять системы информационной безопасности, которые могли бы защитить данные компании. На выбор подходящих средств защиты информации влияют многие факторы, включая сферу деятельности компании, ее размер, техническую сторону, а также знания сотрудников в области информационной безопасности. Если у вас есть вопросы по поводу решений информационной безопасности, которые лучше всего подошли бы для вашего предприятия, а также как их внедрять, обращайтесь к специалистам компании «Пирит».

Литература:

1. Бачило, И. Л. Информационное право : учебник / И. Л. Бачило, В. Н. Лопатин, М. А. Федотов. — СПб. : Юридический центр Пресс, 2005. — 723 с.

2. Городов, О. А. Информационное право : учебник /О. А. Городов. — М. :Проспект, 2006. — 242 с.

3. Копылов, В. А. Информационное право : учебник /В. А. Копылов. — М. :Юристъ, 2005.— 510 с.

4. Правовое обеспечение информационной безопасности : учеб. пособие / под ред. С. Я. Казанцева. — М. : Академия, 2008. — 239 с.

5. Правовое обеспечение информационной безопасности : учебник / В. А. Минаев [и др.]. — 2-е изд., доп. — М. : Маросейка, 20