Конспект лекций проф.Ясенева В.Н. по «Информационной безопасности» для студентов 1 курса по направлению 38.03.01 Экономика и 38.05.01 «Экономическая безопасность»

Введение

Дисциплина «Информационная безопасность» относится к базовой части учебного плана по ряду направлений 38.03.01 «Экономика», 38.05.01 «Экономическая безопасность» обязательна для освоения на 1–м курсе во 2–м семестре. Основное назначение данной дисциплины состоит в эффективном освоении теоретических основ обеспечения информационной безопасности организаций, формирование умения и практических навыков применения методов и средств защиты информации.

В связи с этим, основной задачей преподавания дисциплины «Информационная безопасность» является подготовка экономистов и менеджеров, обладающих знаниями, навыками, умениями в сфере обеспечения информационной безопасности организаций различных форм собственности.

В ходе изучения дисциплины студенты должны комплексно применять знания, навыки и умения, полученные при изучении «Информатики».

Минимальный уровень освоения содержания дисциплины предполагает:

- Знакомство с основными понятиями информационной безопасности, информационными угрозами, их классификацией, и возможными последствиями для организаций различных форм собственности;
- Уяснение вопросов обеспечения информационной проблем создания (концептуального проектирования) систем информационной безопасности;
- Принятие обоснованных решений по выбору политики информационной безопасности (ИБ) и оценки эффективности инвестиций в ИБ.

Содержательные аспекты дисциплины «Информационная безопасность» логически связаны с такими учебными дисциплинами как: «Информатика», «Информационные системы в экономике», «Менеджмент», «Маркетинг», «Финансы», «Бухгалтерский учет» и др.

Тематическим планом преподавания дисциплины предусматриваются следующие виды занятий: лекции, практические занятия, самостоятельная работа. Контроль знаний обучаемых осуществляется в ходе тестирования и сдачи экзамена.

Знания, навыки и умения, приобретенные в процессе изучения дисциплины в ходе лекций, лабораторных занятий и самостоятельной работы, должны всесторонне использоваться студентами на завершающем этапе обучения в бакалавриате, при обучении в магистратуре, а также в процессе дальнейшей профессиональной деятельности при решении широкого класса аналитических задач финансово-экономического характера.

Реализация компетентностного подхода при изучении дисциплины «Информационная безопасность» предполагает широкое использование в учебном процессе активных и интерактивных форм проведения занятий (компьютерных программ, деловых игр по актуальным проблемам, разбор конкретных ситуаций) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков

студентов. В рамках данного курса возможны встречи с представителями компаний различных форм собственности, государственных и муниципальных органов.

Все занятия, проводимые по дисциплине, в том числе и самостоятельная работа студентов, предусматривают сочетание передовых методических приемов с новыми образовательными информационными технологиями.

На занятиях используются современные формы и методы обучения (тренинги, исследовательские методы, проблемное и проектное обучение), направленные на развитие творческих способностей и самостоятельности студентов, привитие им интереса к исследовательской работе, формирование убеждения о необходимости при решении любых прикладных задач использования инновационных информационных технологий.

Лекционные занятия проводятся в специализированных аудиториях с применением мультимедийных технологий и предусматривают развитие полученных теоретических знаний с использованием рекомендованной учебной литературы и других источников информации, в том числе информационных ресурсов сети Интернет.

Практические занятия проводятся в компьютерных классах с применением специализированных информационных систем, комплексов и технологий бизнес-индустрии.

Тематика практических заданий ориентирована на рассмотрение аналитических типовых и исследовательских задач финансово-экономического характера.

В ходе самостоятельной работы, при подготовке к плановым занятиям и экзамену студенты анализируют поставленные преподавателем задачи с использованием учебно-методической литературы, информационных систем, комплексов и технологий, материалов, найденных в глобальной сети Интернет.

Тема 1. Теоретические аспекты информационной безопасности экономических систем

1. Основные понятия информационной безопасности экономического объекта.
2. Экономическая информация как товар и объект безопасности.
   Контрольные вопросы и тесты

1.Основные понятия информационной безопасности экономического объекта

Современное общество называется информационным. Широкое развитие средств вычислительной техники и связи позволило собирать, хранить, обрабатывать и передавать информацию в таких объемах и с такой оперативностью, которые были немыслимы раньше. Благодаря новым информационным технологиям производственная и непроизводственная деятельность человека, его повседневная сфера общения безгранично расширяются за счет вовлечения опыта, знаний и духовных ценностей, выработанных мировой цивилизацией, и сама экономика все в меньшей степени характеризуется как производство материальных благ и все в большей - как распространение информационных продуктов и услуг.

Современный этап информатизации связан с использованием персональной электронно-вычислительной техники, систем телекоммуникаций, создания сетей ЭВМ. Возрастает потребность в разработке и применении эффективных решений в сфере информационной индустрии. Она занимается производством технических и программных средств, информационных технологий для получения новых знаний.

На определенном этапе развития информационной индустрии рождается информационное общество, в котором большинство работающих занято производством, хранением, переработкой и реализацией информации, т.е. творческим трудом, направленным на развитие интеллекта и получение знаний. Создается единое, не разделенное национальными границами информационное сообщество людей.

Формирование информационного общества опирается на новейшие информационные, телекоммуникационные технологии и технологии связи. Именно новые технологии привели к бурному распространению глобальных информационных сетей, открывающих принципиально новые возможности международного информационного обмена. Формирование информационного общества концептуально и практически означает формирование мирового информационного пространства.

Информационное пространство (инфосфера) - сфера человеческой деятельности связанная: с созданием, преобразованием и потреблением информации и включающая в себя:

- индивидуальное и общественное сознание
- информационные ресурсы, то есть информационную инфраструктуру (комплекс организационных структур, технических средств, программного и другого обеспечения для формирования, хранения, обработки и передачи информации), а также собственно информацию и ее потоки.

Глобальная информатизация в настоящее время активно управляет существованием и жизнедеятельностью государств мирового сообщества, информационные технологии применяются при решении задач обеспечения национальной, военной, экономической безопасности и др. Вместе с тем, одним из фундаментальных последствий глобальной

информации государственных и военных структур стало возникновение принципиально новой среды противоборства конкурирующих государств – **киберпространства**, которое не является в общепринятом смысле этого слова, но, тем не менее, в полной мере является международным.

В процессе формирования глобального киберпространства происходит конвергенция военных и гражданских компьютерных технологий. В ведущих зарубежных государствах интенсивно разрабатываются новые средства и методы активного воздействия на информационную инфраструктуру потенциальных противников, создаются различные специализированные кибернетические центры и подразделения управления и командования, основной задачей которых является защита государственных и военных информационных секретов.

Киберпространство – глобальная область информационной среды, включающая в свой состав взаимозависимую совокупность информационно-технической инфраструктуры, в том числе информационные и телекоммуникационные сети и компьютерные системы, предназначенные для хранения, обработки, модификации и обмена данными.

Прогресс в новейших информационных технологиях делает весьма уязвимым любое общество. Каждый прорыв человечества в будущее не освобождает его от груза прошлых ошибок и нерешенных проблем. Когда экономические войны из-за интеграции национальных экономик стали слишком опасными и убыточными, а глобальный военный конфликт вообще способен привести к исчезновению жизни на планете, война переходит в иную плоскость - информационную.

Информационная война (кибервойна) - информационное противоборство с целью нанесения ущерба важным структурам противника, подрыва его политической и социальной систем, а также дестабилизации общества и государства противника.

В современных условиях совершенно справедливо утверждение о том, что война в XXI веке будут гибернетическими. Итак, для любого государства кибербезопасность становится острой и специфической проблемой в обеспечении своей национальной безопасности и защите своих интересов.

В 2014 году Россия вступила в фазу крупномасштабной информационной войны со странами ЕС и США. Ряд информационных всплесков, как известно, был вызван событиями на Украине, сменой власти в Крыму, обвинениями в коррупции и т.п. Помимо чисто политических, имеется и ряд формальных причин, например, в сфере спорта. В результате взаимное противостояние переместилось на информационную плоскость.

Сфера использования информационного оружия – массовые сообщения в СМИ, по каналам спецслужб, в Internet и т.д. Соответствующая информация предоставляется в подавляющем большинстве случаев как бездоказательные факты, а тактикой информационных атак является многократное повторение желаемой установки. Что требует применения адекватных мер со стороны российских властей.

Помимо удара по репутации государства, было нарушено международное взаимодействие. Что привело к ухудшению инвестиционного климата. Росту оттока капиталов, выход с российского рынка ряда иностранных компаний, в конечном счете, снижению уровня жизни граждан. Информационные атаки нанесли существенный ущерб в особенности на финансовых рынках. Так, 25 апреля 2014 года рейтинговые агентства Standard & Poor's понизило суверенный рейтинг России с «BBB-»до «BBB» с рейтингом

«негативный», что вызвало девальвацию рубля, подавляющего большинства котировок российского рынка акций.

Информационное противоборство - форма межгосударственного соперничества, реализуемая посредством оказания информационного воздействия на системы управления других государств и их вооруженных сил, а также на политическое и военное руководство и общество в целом, информационную инфраструктуру и средства массовой информации этих государств для достижения выгодных для себя целей при одновременной защите от аналогичных действий от своего информационного пространства.

Информационная преступность - проведение информационных воздействий на информационное пространство или любой его элемент в противоправных целях. Как ее частный вид может рассматриваться информационный терроризм, то есть деятельность, проводимая в политических целях.

Информационное воздействие - акт применения информационного оружия.

Информационное оружие (кибероружие) - комплекс технических и других средств, методов и технологий, предназначенных для:

- установления контроля над информационными ресурсами потенциального противника;
- вмешательство в работу его систем управления и информационных сетей, систем связи и т.п. в целях нарушения их работоспособности, вплоть до полного выведения из строя, изъятия, искажения содержащихся в них данных или направленного введения специальной информации;
- распространение выгодной информации и дезинформации в системе формирования общественного мнения и принятия решений;
- воздействие на сознание и психику политического и военного руководства, личного состава вооруженных сил, спецслужб и населения противостоящего государства, используемых для достижения превосходства над противником или ослабления проводимых им информационных воздействий.

Активное развитие информационных технологий обуславливает актуальность изучения проблем информационной безопасности: угроз для информационных ресурсов, различных средств и мер защиты, барьеров для проникновения, а также уязвимостей в системах защиты информации. Под информационной безопасностью в более общем виде следует понимать совокупность средств, методов и процессов (процедур), обеспечивающих защиту информационных активов и, следовательно, гарантирующих сохранение эффективности и практической полезности как технической инфраструктуры информационных систем, так и сведений, которые в таких системах хранятся и обрабатываются.

Под **угрозой безопасности информации** понимаются события или действия, которые могут привести к искажению, несанкционированному использованию или даже к разрушению информационных ресурсов управляемой системы, а также программных и аппаратных средств.

Если исходить из классического рассмотрения кибернетической модели любой управляемой системы, возмущающие воздействия на нее могут носить случайный характер. Поэтому среди угроз безопасности информации следует выделять как один из видов угроз случайные, или непреднамеренные. Их источником могут быть выход из строя аппаратных средств, неправильные действия работников информационные системы (ИС) или ее пользователей, непреднамеренные ошибки в программном обеспечении и т.д.

Такие угрозы тоже следует держать во внимании, т.к. ущерб от них может быть значительным. Однако в данной работе наибольшее внимание уделяется угрозам умышленным, которые в отличие от случайных преследуют цель нанесения ущерба управляемой системе или пользователям. Это делается нередко ради получения личной выгоды.

Человека, пытающегося нарушить работу информационной системы или получить несанкционированный доступ к информации, обычно называют "компьютерным пиратом" (хакером).

В своих противоправных действиях, направленных на овладение чужими секретами, взломщики стремятся найти такие источники конфиденциальной информации, которые бы давали им наиболее достоверную информацию в максимальных объемах с минимальными затратами на ее получение. С помощью различного вида уловок и множества приемов и средств подбираются пути и подходы к таким источникам. В данном случае под источником информации понимается материальный объект, обладающий определенными сведениями, представляющими конкретный интерес для злоумышленников или конкурентов.

Кибербезопасность – это свойство или состояние системы сохранять надежность и функциональную устойчивость в условиях современного информационного противоборства.

Кибербезопасность – информационная безопасность компьютерных информационно-управляющих систем, обеспечивающая их высокую надежность и функциональную устойчивость в условиях современного информационного противоборства. *Или, иначе, кибербезопасность – это информационная безопасность в компьютерной инфосфере в условиях современного информационного противоборства.*

Кратко, кибербезопасность – это безопасность в киберпространстве.

Информационная безопасность включает:

✓ состояние защищенности информационного пространства, обеспечивающее его формирование и развитие в интересах граждан, организаций и государства;

✓ состояние инфраструктуры, при котором информация используется строго по назначению и не оказывает негативного воздействия на систему при ее использовании;

✓ состояние информации, при котором исключается или существенно затрудняется нарушение таких ее свойств, как конфиденциальность, целостность и доступность;

✓ экономическую составляющую (структуры управления в экономической сфере, включая системы сбора, накопления и обработки информации в интересах управления производственными структурами, системы общеэкономического анализа и прогнозирования хозяйственного развития, системы управления и координации в промышленности и на транспорте, системы управления энергосистем, централизованного снабжения, системы принятия решения и координации действий в чрезвычайных ситуациях, информационные и телекоммуникационные системы);

✓ финансовую составляющую (информационные сети и базы данных банков и банковских объединений, системы финансового обмена и финансовых расчетов).

Обеспечение информационной безопасности должно начинаться с выявления субъектов отношений, связанных с использованием информационных систем. Спектр их интересов может быть разделен на следующие основные категории: доступность (возможность за приемлемое время получить требуемую информационную услугу), целостность (актуальность и непротиворечивость информации, ее защищенность от

разрушения и несанкционированного изменения), конфиденциальность (защита от несанкционированного ознакомления).

Исходя из вышеизложенного, в наиболее общем виде информационная безопасность может быть определена как невозможность нанесения вреда свойствам объекта безопасности, обусловливаемым информацией и информационной инфраструктурой (рис. 1).

Рис. 1 Структура понятия «Информационная безопасность»

Понятие информационной безопасности в узком смысле этого слова подразумевает:

- надежность работы компьютера;
- сохранность ценных данных;
- защиту информации от внесения в нее изменений неуполномоченными лицами;
- сохранение тайны переписки в электронной связи.

Безопасность проявляется как невозможность нанесения вреда функционированию и свойствам объекта, либо его структурным составляющим.

Объектом информационной безопасности может быть коммерческое предприятие. Тогда содержание "информационной безопасности" будет заключаться в защищенности интересов собственника данного предприятия, удовлетворяемых с помощью информации, либо связанных с защитой от несанкционированного доступа тех сведений, которые представляются собственнику достаточно важными. Интересы проявляются через объекты, способные служить для их удовлетворения, и действия, предпринимаемые для обладания этими объектами. Соответственно интересы как объект безопасности могут быть представлены совокупностью информации, способной удовлетворять интерес собственника, и его действий, направленных на овладение информацией или сокрытие информации. Эти составляющие объекта информационной безопасности и защищаются от внешних и внутренних угроз.

К объектам информационной безопасности на предприятии относят:

❖ информационные ресурсы, содержащие сведения, отнесенные к коммерческой тайне, и конфиденциальную информацию, представленную в виде информационных массивов и баз данных;

❖ средства и системы информатизации - средства вычислительной и организационной техники, сети и системы, общесистемное и прикладное программное обеспечение, автоматизированные системы управления предприятиями, системы связи и передачи данных, технические средства сбора, регистрации, передачи, обработки и отображения информации, а также их информативные физические поля.

При осуществлении коммерческой деятельности возникает информация, известность которой другим участникам рынка может существенно снизить доходность этой деятельности. В деятельности государства порождается информация, раскрытие которой может снизить эффективность проводимой политики. Подобная информация закрывается, и устанавливаемый режим ее использования призван предупредить возможность несанкционированного ознакомления с ней. В этом случае объектом безопасности выступает режим доступа к информации, а информационная безопасность заключается в невозможности нарушения этого режима. Примером могут служить информационно-телекоммуникационные системы и средства связи, предназначенные для обработки и передачи сведений, составляющих государственную тайну. Основным объектом безопасности в них является режим доступа к секретной информации. Информационная безопасность таких систем заключается в защищенности этой информации от несанкционированного доступа, уничтожения, изменения и других действий. Система обеспечения безопасности информации включает подсистемы:

- компьютерную безопасность;
- безопасность данных;
- безопасное программное обеспечение;
- безопасность коммуникаций.

Компьютерная безопасность обеспечивается комплексом технологических и административных мер, применяемых в отношении аппаратных средств компьютера с целью обеспечения доступности, целостности и конфиденциальности, связанных с ним ресурсов.

Безопасность данных достигается защитой данных от неавторизованных, случайных, умышленных или возникших по халатности модификаций, разрушений или разглашении.

Безопасное программное обеспечение представляет собой общесистемные и прикладные программы и средства, осуществляющие безопасную обработку данных и безопасно использующие ресурсы системы.

Безопасность коммуникаций обеспечивается принятием мер по предотвращению предоставления неавторизованным лицам информации, которая может быть выдана системой в ответ на телекоммуникационный запрос.

Политика безопасности включает в себя анализ возможных угроз и выбор соответствующих мер противодействия, являющихся совокупностью тех норм, правил поведения, которыми пользуется конкретная организация при обработке информации и ее защите.

Угроза безопасности информации - события или действия, которые могут привести к искажению, неразрешенному использованию или к разрушению информационных ресурсов управления системы, а также программных и аппаратных средств.

Защита информации (ЗИ) - комплекс мероприятий, направленных на обеспечение важнейших аспектов информационной безопасности: целостности, доступности и, если нужно, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных.

Основные предметные направления ЗИ - охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности.

Система - это совокупность взаимосвязанных элементов, подчиненных единой цели.

Признаками системы являются следующие:

1. Элементы системы взаимосвязаны и взаимодействуют в рамках системы.
2. Каждый элемент системы может в свою очередь рассматриваться как самостоятельная система, но он выполняет только часть функций системы.
3. Система как целое выполняет определенную функцию, которая не может быть сведена к функциям отдельно взятого элемента.
4. Подсистемы могут взаимодействовать как между собой, так и с внешней средой и изменять при этом свое содержание или внутреннее строение.

Под системой безопасности будем понимать организованную совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих защиту жизненно важных интересов личности, предприятия и государства от внутренних и внешних угроз.

Система защиты информации представляет организованную совокупность специальных органов, средств, методов и мероприятий, обеспечивающих защиту информации от внутренних и внешних угроз

С позиций системного подхода к защите информации предъявляются определенные требования:

- обеспечение безопасности информации не может быть одноразовым актом. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных методов, способов и путей совершенствования и развития системы защиты, непрерывном контроле ее состояния, выявления ее узких и слабых мест и противоправных действий;
- безопасность информации может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты во всех структурных элементах экономической системы и на всех этапах технологического цикла обработки информации;
- планирование безопасности информации осуществляется путем разработки каждой службой детальных планов защиты информации в сфере ее компетенции;
- защите подлежат конкретные данные, объективно подлежащие охране, утрата которых может причинить организации определенный ущерб;
- методы и средства защиты должны надежно перекрывать возможные пути неправомерного доступа к охраняемым секретам;
- эффективность защиты информации означает, что затраты на ее осуществление не должны быть больше возможных потерь от реализации информационных угроз;
- четкость определения полномочий и прав пользователей на доступ к определенным видам информации;
- предоставление пользователю минимальных полномочий, необходимых ему для выполнения порученной работы;
- сведение к минимуму числа общих для нескольких пользователей средств защиты;

- учет случаев и попыток несанкционированного доступа к конфиденциальной информации; обеспечение степени конфиденциальной информации;
- обеспечение контроля целостности средств защиты и немедленное реагирование на их выход из строя.

Система защиты информации, как любая система, должна иметь определенные виды собственного обеспечения, опираясь на которые она будет выполнять свою целевую функцию. С учетом этого система защиты информации имеет:

правовое обеспечение. Сюда входят нормативные документы, положения, инструкции, руководства, требования которых являются обязательными в рамках сферы действия;

организационное обеспечение. Имеется в виду, что реализация защиты информации осуществляется определенными структурными единицами, такими как: служба безопасности, служба режима, служба защиты информации техническими средствами и др.

аппаратное обеспечение. Предполагается широкое использование технических средств, как для защиты информации, так и для обеспечения деятельности собственно системы защиты информации;

информационное обеспечение. Оно включает в себя документированные сведения (показатели, файлы), лежащие в основе решения задач, обеспечивающих функционирование системы. Сюда могут входить как показатели доступа, учета, хранения, так и системы информационного обеспечения расчетных задач различного характера, связанных с деятельностью службы обеспечения безопасности;

программное обеспечение. К нему относятся антивирусные программы, а также программы (или части программ регулярного применения), реализующие контрольные функции при решении учетных, статистических, финансовых, кредитных и других задач;

математическое обеспечение. Предполагает использование математических методов для различных расчетов, связанных с оценкой опасности технических средств злоумышленников, зон и норм необходимой защиты;

лингвистическое обеспечение. Совокупность специальных языковых средств общения специалистов и пользователей в сфере защиты информации;

нормативно-методическое обеспечение. Сюда входят нормы и регламенты деятельности органов, служб, средств, реализующих функции защиты информации, различного рода методики, обеспечивающие деятельность пользователей при выполнении своей работы в условиях жестких требований защиты информации;

эргономическое обеспечение. Совокупность средств, обеспечивающих удобства работы пользователей аппаратных средств защиты информации.

КИБЕРБЕЗОПАСНОСТЬ - ПОДХОДЫ К ОПРЕДЕЛЕНИЮ ПОНЯТИЯ

Безкоровайный Михаил Михайлович, *кандидат технических наук, доцент*
Татузов Александр Леонидович, *доктор технических наук, доцент*

Существенный рост инцидентов, возникающих в информационной сфере, привел к необходимости системного анализа источников возникновения угроз. Для этого необходимы согласованные среди специалистов понятия, ключевым из которых является кибербезопасность. Оно трактуется неоднозначно многими экспертами. В статье

предлагается подход к рассмотрению понятия киберпространства и кибербезопасности.

Ключевые слова: *информационная безопасность, кибербезопасность, киберпространство, киберпреступления.*

CYBERSECURITY - APPROACHES TO THE DEFINITION

Mikhail Bezkorovainy, *Ph.D., Associate Professor* ***Alexander Tatuzov,*** *Doctor of Technical Sciences, Associate Professor*

Many experts treat this concept in different ways. The paper proposes an approach to the consideration of cyberspace and cybersequrity.

Keywords: *information security, cybersecurity, cyberspace, cybercrime.*

В настоящее время наблюдается резкий рост инцидентов в области информационной безопасности, которые имеют широкое распространение и приобретают угрожающий характер. Многие из подобных атак затрагивают широкий круг частных, корпоративных, а также государственных интересов.

Главными тенденциями развития угроз являются следующие:

- рост числа атак, многие из которых ведут к большим потерям;
- возрастание сложности атак, которые могут включать несколько этапов и применять специальные методы защиты от возможных методов противодействия;
- воздействие практически на все электронные (цифровые) устройства, в числе которых в последнее время все большую значимость приобретают мобильные устройства, а они в наибольшей степени подвержены рискам в области информационной безопасности;
- все более частые случаи нападения на информационную инфраструктуру крупных корпораций, важнейших промышленных объектов и даже государственных структур;
- применение наиболее развитыми в области компьютерных технологий странами средств и методов кибернападения на другие государства.

Это подтверждается практически ежедневными сводками новостей, в которых сообщается о новых атаках преступников в информационной сфере.

Число вредоносных объектов, которые обнаруживаются в сети ежегодно, исчисляется миллиардами, их распространение ведется более чем 100 миллионов интернет адресов [1] [2]. Каждый год это число увеличивается на 40% [3]. Атаки в информационном пространстве наносят ущерб, который оценивается в 100 миллиардов долларов [4]. По заявлению начальника Бюро специальных технических мероприятий МВД России Алексея Мошкова каждую секунду 12 человек на Земле становятся жертвами киберпреступников. Только в России удалось предотвратить хищение около 1 миллиарда рублей с банковских счетов граждан [5].

Особую опасность составляют угрозы мобильным устройствам, которые ранее редко подвергались атакам. За один год практически в 30 раз увеличилось количество Android-троянцев [3].

Появились крайне сложные элементы нападения, направленные на ухудшение работы промышленных объектов. Это обнаруженный в 2009 г., и наделавший много шума червь Stuxnet, разработки этого года Duqu и Flame, последний из которых имеет очень сложную архитектуру. Стало известно о причастности специалистов американских спецслужб к созданию этих комплексных вредоносных программ. Государственными

структурами ведется финансирование нападений в области киберпространства [6].

Зафиксированы многочисленные атаки на крупнейшие банки США. Эти атаки смогли взломать передовые системы защиты и создать угрозы национальной инфраструктуре. Предположительно, нападения чаще всего организуются из Китая [7]. В начале года была проведена серия атак на крупнейшие американские СМИ [8], что заставило правительство США еще раз серьезно задуматься об усилении кибербезопасности в стране [9].

В 2013 г. Лабораторией Касперского была опубликована информация о совершенно новом явлении в области компьютерных атак. Была раскрыта шпионская сеть «Красный Октябрь (Red October)*, на протяжении пяти лет занимающаяся хищением государственных секретов. Это сложнейший комплекс вредоносных программ, около 1000 вредоносных файлов, относящихся к 30 различным группам модулей [10]. Аналогичные методы уже активно применяются и для мобильных устройств на платформе Android [11].

В конце 2012 г. американские и китайские государственные структуры публично высказали свои подозрения в создании оборудования с недокументированными возможностями, посредством которых из одного государства были атакованы сети другой страны. Под подозрением оказалась продукция фирм Huawei и ZTE с китайской стороны и Cisco с американской стороны [12].

Заявления Эдварда Сноудена подтверждают активное участие государственных структур развитых стран в сборе информации о гражданах, чиновниках, корпорациях и других, казалось бы, общедоступных сведений, которые можно агрегировать для достижения кумулятивного эффекта и получения закрытой информации. С целью манипулирования общественным мнением масс людей активно применяются специальные методы социальной инженерии, во многом опирающиеся на средства коммуникаций с помощью Интернета.

Таким образом, имеется ряд проблем в сфере информационной безопасности, которые не могут быть полноценно решены традиционными средствами и на которые следует обратить внимание обществу и государственным органам. Масштабные нарушения, затрагивающие все стороны жизни общества, в основе которых лежат новейшие методы осуществления атак на компьютерные сети, а также управление общественным сознанием требуют системного подхода к созданию комплексной системы безопасности, способной противостоять этим угрозам.

Общий анализ проблематики защиты от подобных, вновь возникающих и продолжающих развиваться угроз, можно обозначить понятием кибербезопасность. Вопросы обеспечения кибербезопасности были проанализированы в работе [13] и была показана необходимость принятия масштабных мер со стороны государства по обеспечению безопасности в области информационных и телекоммуникационных технологий (далее - ИКТ). Речь идет о координации усилий в этом направлении государственных органов, бизнеса и общества в целом.

Столь сложная задача должна решаться на основе ясно выработанной позиции, однозначном понимании того, что имеется в виду под кибербезопасностью. В работе [14] рассмотрены подходы к выработке терминологии в этой области.

Очевидно, что кибербезопасность должна быть нацелена на обеспечение защиты в киберпространстве. Поэтому основным для анализа проблем кибербезопасности является понятие киберпространство.

Для понимания его содержания целесообразно основываться на термине

кибернетика. Кибернетика (от греч. «искусство управления») - наука об управлении, связи и переработке информации.

Абстрактная кибернетическая система представляет собой множество взаимосвязанных объектов, называемых элементами системы, способных воспринимать, хранить и перерабатывать информацию, а также обмениваться информацией. То есть, к предметной области кибернетики относятся все современные информацибнные и телекоммуникационные технологии. Важно, что в рамках кибернетического подхода элементы системы рассматриваются как непрерывно взаимодействующие между собой и в качестве важных составляющих элементов в киберпространство включены люди - активные участники информационного обмена и использования информационных ресурсов.

В начале 2014 г. Советом Федерации для публичного обсуждения был предложен проект Концепции Стратегии кибербезопасности Российской Федерации (далее - Концепция). Он призван определить направления усилий государства в отношении новых угроз, возникающих в современном информационном мире [15].

Понятие кибербезопасности очень многогранно и поэтому непросто и трудно формализуемо. Здесь существует очень много различных представлений и взглядов.

Специалисты по информационной безопасности и просто заинтересованные пользователи, в частности, те, которые оставили комментарии к Концепции, высказывают очень противоречивые взгляды на эту проблематику. Анализ комментариев показывает, что одной из основных проблем разработки подобных документов заключается в трудности понимания термина киберпространство и соотнесенным с ним понятием кибербезопасность.

Киберпространство в проекте Концепции определяется следующим образом:

«Киберпространство - сфера деятельности в информационном пространстве, образованная совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства)».

В принципе, такое определение в какой-то степени трактует отдельные аспекты этого важного понятия, но отсутствие дальнейших подробных разъяснений приводит к неточному его пониманию. Абсолютное большинство экспертов, которые оставили свои комментарии к проекту Концепции, считают, что в определении речь идет исключительно 6 технологической составляющей информационного поля, то есть о компьютерной и телекоммуникационной инфраструктуре. Совсем упущен из рассмотрения вопрос о деятельности на основе этой инфраструктуры и любых видах человеческой активности, которая осуществляется посредством технологий. А об этом прямо сказано в определении. Для документа, имеющего столь важное значение это неприемлемо и указывает на необходимость дальнейшей методологической работы по определению кибербезопасности как характеристики киберпространства.

Приведенное в концепции определение во многом перекликается с позицией международного стандарта ИСО/МЭК 27032:2012 Руководящие указания по кибербезопасности (ISO/ IEC 27032:2012 Information technology - Security techniques - Guidelines for cybersecurity).

Киберпространство - это сложная среда, не существующая ни в какой физической форме, возникающая в результате взаимодействия людей, ПО, интернет сервисов

посредством технологических устройств и сетевых связей.

В программной статье по кибербезопасности специалистами Великобритании определяется это понятие как *всякая деятельность в сетевой, цифровой форме,* добавляя после этого, что *сюда же относятся информационное содержание и действия осуществляемые посредством цифровых сетей.* (Klimburg A. et al. National cyber security framework manual //NATO CCD COE Publications (December 2012). - 2012. http://belfercenter.hks. harvard.edu/files/hathaway-klimburg-nato-manual-ch-1.pdf).

При всем многообразии этих определений можно отметить, что при четком указании на связанность киберпространства с ИКТ инфраструктурой, основное внимание обращено не на технологии, а на деятельность людей, которые используют эти технологии.

Важно, что основное содержание киберпространства заключается в деятельности пользователей цифровыми информационными ресурсами и ИКТ инфраструктурой. Киберпространство можно рассматривать как триаду, которая включает в себя три основные составляющие.

Информация в ее цифровом представлении: статическом (файлы, записанные на носители данных) и динамическом (пакеты, потоки, команды, запросы, и т.д. передаваемые по различным сетям, обрабатываемые в автоматизированных системах и представляемые на средствах отображения в графическом или текстовом виде).

Техническая инфраструктура, ИКТ, программное обеспечение, с помощью которых осуществляется реализация основных действий с информацией: сбор, обработка, хранение и передача. К таким средствам относятся инфраструктура Интернет и сетевых взаимосвязей, компьютеры, всевозможные гаджеты и т.п.

Информационное взаимодействие субъектов с использованием информации получаемой (передаваемой) и обрабатываемой посредством технической инфраструктуры. Здесь имеются в виду все виды деятельности пользователей или участников киберпространства, которые они осуществляют с использованием информационных ресурсов, потоки и хранилища которых располагаются на технической инфраструктуре.

Все эти составляющие в совокупности и образуют сущность, которую можно именовать киберпространством. Можно выделить следующие его основные свойства.

Первое. Киберпространство определено на множестве цифровых устройств и систем на их основе, которые оперируют с информацией или во многом с ее помощью. Важно, что имеются в виду не отдельные системы, а их совокупность, когда подобных устройств (систем) достаточно много. То есть, в общем виде существенное уменьшение числа функционирующих устройств (систем) в киберпространстве или нарушение их нормальной работы является угрозой киберпространству. Но речь идет не просто об отдельных устройствах (системах), а о большом числе таких объектов и способности оперировать ими информацией (обеспечивать сервисы) с заданным качеством, то есть осуществлять действия, которые обычно связываются с информационными технологиями. Отсюда вытекает второе свойство.

Активное оперирование информацией и сохранение этой информацией главных ее свойств: целостности, доступности, конфиденциальности и других, определяемых в современных стандартах. В отличие от информационной безопасности речь идет не об информации вообще, а о той информации, которая циркулирует в киберпространстве и составляет важную часть ее содержания. Таким образом, нарушение работы отдельного компьютера подключенного к киберпространству или утеря информации, которая в нем содержится, или нарушение ее свойств, безусловно важных для пользователя данного

компьютера, вряд ли может рассматриваться как угроза кибербезопасности.

Третье. Наличие «добропорядочных» связей, связей, которые составляют основу киберпространства, и без которых рассматривать поле цифровых устройств (систем) в качестве некоторой новой сущности вряд ли имело бы смысл. Здесь имеется в виду способность киберпространства передавать, получать и обрабатывать информацию с сохранением ее существенных для целей применения свойств.

Четвертое. Собственно понятие кибер-. Оно относится к управлению. Управление в данном случае подразумевает не наличие прямолинейных команд, которые непосредственно исполняются всеми агентами (участниками) киберпространства, а формирование и передача таких сигналов, которые способны придать рассматриваемой области киберпространства некий «разумный» характер поведения и устойчивость к возникающим угрозам.

Способы управления оказывают непосредственное воздействие на структуру киберпространства. Здесь важно учитывать управление технической основой киберпространства и чисто физическими связями между отдельными узлами или даже областями киберпространства. Но определяющую роль играет управление участниками киберпространства: пользователями и их группами. Под управлением понимается комплекс усилий, направленный на повышение квалификации участников, стимулирование благоприятных для развития киберпространства действий и подавление или прямое запрещение злонамеренных действий. Управление субъектами киберпространства играет определяющую роль в возникновении, существовании и поддержке основных свойств этого образования.

Указанные свойства, а именно многочисленность элементов, составляющих киберпространство, обилие взаимосвязей между ними, возможность применения специальных техник управления действиями этих элементов, и определяют развитие тех угроз, о которых говорилось выше. Необыкновенно высокая и все нарастающая интенсивность атак происходит от громадных масштабов киберпространства, всевозможных и разнохарактерных связей между ними. Сложные атаки, имеющие комплексную структуру, опираются на возможность различных направлений распространения информации и сигналов. Использование методов социальной инженерии позволяет изыскивать наиболее продуктивные методы организации атак. В киберпространстве могут развиваться все более опасные и сложные угрозы. Они используют особенности его построения для достижения максимального эффекта.

Но те же самые особенности, проистекающие из многочисленных взаимосвязей между участниками киберпространства, могут стать важным фактором в повышении эффективности систем, которые обеспечивают защиту от подобных угроз [16]. Для этого необходимо координировать усилия всех заинтересованных участников, создавать механизмы, способствующие наилучшему распределению их усилий. Нужно правильно определять возникающие и прогнозируемые опасности и обоснованно выбирать рациональные меры защиты.

Кибербезопасность имеет целью решение этих вопросов и обеспечение нормального функционирования киберпространства, защищая его от возникающих угроз эффективным образом.

Важно правильно сформулировать понятие кибербезопасности, чтобы главные цели работы служб и средств защиты киберпространства от возникающих угроз были точно определены. Однако в концепции приведена формулировка, которая не может

удовлетворить этим требованиям.

В проекте Концепции говорится следующее:

«кибербезопасность - совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями».

Кибербезопасность не может быть направлена на защиту от максимального числа угроз. Нужно обеспечить максимально благоприятную среду для работы пользователей и всех систем в киберпространстве.

Указанная в Концепции постановка неявно призывает разрабатывать и выявлять все новые и новые угрозы, создавая новые средства и способы защиты от них.

Доля ресурсов, необходимых для обеспечения защиты, при таком подходе будет неуклонно расти, а устойчивая работа киберпространства может даже ухудшаться.

Поэтому в определении кибербезопасности основной упор и целевая установка должны быть сделаны на сохранение благоприятного состояния киберпространства, а не на число угроз. Если мы смогли защититься от невообразимо большого числа угроз, но работоспособность киберпространства нарушена, то это хуже, чем защититься от двух десятков угроз и при этом сохранить приемлемый уровень работоспособности.

Кибербезопасность так же, как и киберпространство может описываться триадой составляющих ее сущностей определенных на составных частях киберпространства: информационных ресурсах, компьютерной и сетевой архитектурах (инфраструктуре) и способах взаимодействия пользователей.

Кибербезопасность охватывает уже не только информацию как объект защиты, не исключительно технические средства, которые определяют возможности функционирования информации, а защиту способов функционирования новой сущности - киберпространства. Защищается деятельность людей, которая осуществляется с помощью информации, распространяемой посредством технической инфраструктуры ИКТ.

При обеспечении кибербезопасности важно учитывать указанные особенности киберпространства и ее наиболее важный аспект - наличие взаимосвязей между участниками (пользователями), что приводит к возможности возникновения синергетического эффекта.

В проекте Концепции указывается на необходимость проведения научных исследований в области кибербезопасности, в частности, на реализацию научно-технических программ и исследований в соответствии с «Приоритетными направлениями научных исследований в области обеспечения информационной безопасности Российской Федерации», утвержденными Советом Безопасности Российской Федерации. Но это лишь общая постановка, отсылающая к списку из более 100 направлений, среди которых необходимо выделить наиболее значимые с точки зрения кибербезопасности. На этих направлениях стоит сосредоточить основные усилия. Предложения по таким работам приведены в статье [17]. Кроме того, следует дополнить тематику перспективных исследований направлениями, которые вытекают из основных свойств киберпространства.

Необходимо подробно и тщательно исследовать основные свойства киберпространства, динамику его развития в различных масштабах времени от мгновенных до многолетних, методы управления этой динамикой. Важно обосновать подходы к определению показателей кибербезопасности, разработать модели для их оценки, выработать способы обоснования критериев.

Без проведения системного анализа и получения оценок применения тех или иных

мер невозможно построить эффективную систему кибербезопасности.

Представляется целесообразным в комплекс исследований в области кибербезопасности включить следующие направления:

1. Выработка единой терминологии киберпространства и кибербезопасности, гармонизированной с существующей терминологией в области информационной безопасности.

2. Разработка комплексной системы показателей, охватывающих все стороны функционирования киберпространства и обеспечения его защиты от возможных угроз.

3. Разработка моделей самого киберпространства и основных факторов, оказывающих влияние на его функционирование. Безусловно, необходима тщательно продуманная модель угроз. Одним из важнейших направлений является создание математических моделей, позволяющих получать численные характеристики информационной безопасности (степени угроз информационной безопасности, анализа информационных рисков, оценки эффективности мер защиты).

4. Создание специальных методов обеспечения устойчивости киберпространства или его областей при воздействии угроз. Здесь несколько возможным тем:

- анализ топологической структуры и выработка рекомендаций по ее изменению, способов и конкретных алгоритмов их реализации;
- новые методы криптографической защиты, основанные не только на чисто вычислительных механизмах реализации стойкости, но и на использовании преимуществ многосвязной архитектуры связей и большого числа добропорядочных пользователей;
- методы информационной безопасности на основе социальных сервисов для противодействия кибератакам с применением специальных процедур анализа группового поведения.

5. Интеллектуальные методы обеспечения кибербезопасности:

- методы интеллектуальной идентификации пользователей;
- интеллектуальные методы предотвращения вирусных и других атак;
- интеллектуальные методы выявления атак и проникновений;
- методы ситуационного анализа состояния информационной безопасности;
- новые методы криптографической защиты, основанные на нейросетевых технологиях.

2.Экономическая информация как товар и объект безопасности

В экономической науке и практике информация, данные, сообщения, знания зачастую используются как синонимы. Но это не одно и тоже. В кибернетике понятие информация определяется: как степень устранения неопределенности знаний у пользователя. С философских позиций информация связана со свойством материи к отражению, а значит информация – это сущность такого отражения, а данные (сообщения) форма проявления этой сущности.

Обычными методами человечество не в состоянии обработать возрастающие объемы цифровой информации (рисунок 2).

Рис. 2. Цифровой потоп (по материалам конференции «Что нас ждет в будущем?», ноябрь 2017 г. Финансовый университет при Правительстве РФ)

Экономическая информация относится к области экономических знаний. Она характеризует процессы снабжения, производства, распределения и потребления материальных благ.

Управление экономическими объектами всегда связано с преобразованием экономической информации.

С кибернетических позиций любой процесс управления сводится к взаимодействию управляемого объекта (им может быть станок, цех, отрасль) и системы управления этим объектом. Последняя получает информацию о состоянии управляемого объекта, соотносит ее с определенными критериями (планом производства, например), на основании чего вырабатывает управляющую информацию (рисунок 3).

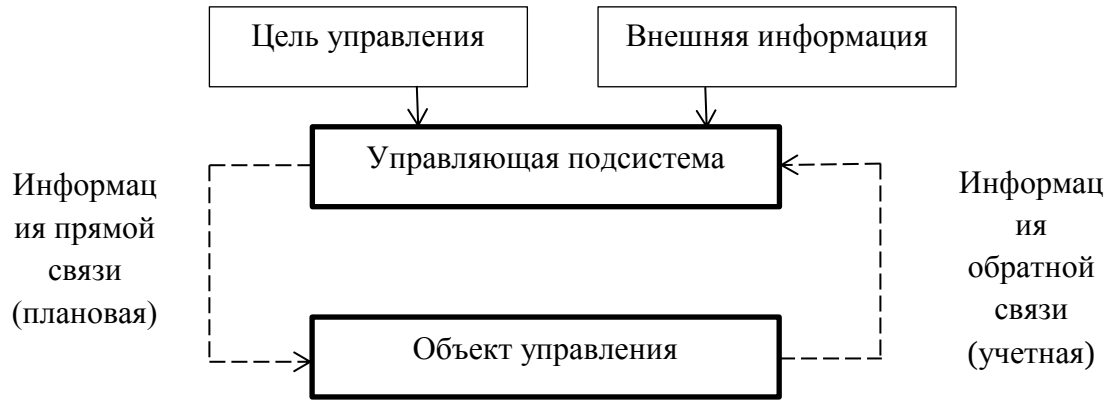

Рис. 3. Кибернетическая модель системы управления

Очевидно, что управляющие воздействия (прямая связь) и текущее состояние управляемого объекта (обратная связь) - не что иное, как информация. Реализация этих процессов и составляет основное содержание работы управленческих служб, включая и экономические.

В деятельности любой фирмы присутствует ***информационный ресурс*** - это документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных и др. информационных системах), т.е. документированные знания. Информационные ресурсы в современном обществе играют не меньшую, а нередко и большую роль, чем ресурсы материальные. Знание - кому, когда и где продать товар может цениться на меньше, чем товар, и в этом плане динамика развития общества свидетельствует о том, что на "весах" материальных и информационных ресурсов последние начинают преобладать. Причем тем сильнее, чем белее общество открыто, чем более развиты в нем средства коммуникации, чем большей информацией оно располагает.

Информационные ресурсы являются исходной для создания ***информационных продуктов.*** Последние являются результатом интеллектуальной деятельности человека и распространяются с помощью услуг.

Посредством информационных услуг осуществляется получение и предоставление в распоряжение пользователя информационных продуктов.

Юридической основой этой операции должен быть договор между двумя сторонами - поставщиком и потребителем, а источником информационных услуг - ***базы данных.*** Они могут существовать в компьютерном и некомпьютерном вариантах, в виде библиографических и небиблиографических взаимосвязанных данных, основанных на общих правилах описания, хранения и манипулирования данными.

Если информационные ресурсы, продукты и услуги, представляют ценность для предметной деятельности, то они являются товаром, за исключением случаев, предусмотренных законодательством РФ.

Информация как всякий товар, имея потребительскую стоимость, обладает рядом особенностей, отличающих ее от товаров, например, продуктов питания, которые при потреблении, как известно, исчезают.

К числу особенностей информации как товара следует отнести:

- **неисчерпаемость** - по мере развития общества и роста потребления ее запасы не убывают, а растут;

- **сохраняемость-** при использовании не исчезает и даже может увеличиваться за счет трансформации полученных сообщений;

- **несамостоятельность** - проявляет свою "движущую силу" только в соединении с другими ресурсами (труд, техника, сырье, энергия).

Следующим важнейшим свойством информации, как товара, является ее цена, формирующаяся на рынке под воздействием, в основном, спроса и предложения. Например, цена на программу "1С-Предприятие" формируется, исходя из затрат на разработку этого информационного продукта, его качества, а также ожидаемого спроса на него. Предложение этого товара может быть обеспечено без каких-либо ограничений в нужном количестве экземпляров в отличие от товарно-материальных ресурсов, которые, как известно, со временем истощаются.

Если информация представляет ценность для организации, то необходимо эту ценность не только использовать, но и защищать.

Цена информации в предпринимательской деятельности может также определяться, как величина ущерба, который может быть нанесен фирме в результате использования коммерческой информации конкурентами. Или наоборот прибыли (дохода), который может быть получен фирмой в результате использования коммерческой информации при принятии управленческих решений.

Информация может использоваться в организации, если удовлетворяет следующим требованиям: конфиденциальность, целостность, оперативность использования (доступность) и достоверность.

Информация может составлять коммерческую тайну, если она отвечает следующим требованиям (критерии правовой охраны):

- к ней нет свободного доступа на законном основании;
- обладатель информации принимает меры к охране ее конфиденциальности.

К коммерческой тайне не может быть отнесена информация:

- содержащаяся в учредительных документах;
- содержащаяся в документах, дающих право заниматься предпринимательской деятельностью (регистрационные удостоверения, лицензии и т.д.)
- содержащаяся в годовых отчетах, бухгалтерских балансах, формах государственных статистических наблюдений, аудиторских заключений, а также в иных, связанных с исчислением и уплатой налогов;
- содержащая сведения об оплачиваемой деятельности государственных служащих;
- содержащаяся в годовых отчетах фондов об использовании имущества;
- связанная с соблюдением экологического и антимонопольного законодательства, обеспечением безопасных условий труда, реализацией продукции, причиняющей вред здоровью населения;
- о деятельности благотворительных организаций и некоммерческих организаций, не связанных с предпринимательской деятельностью;
- о наличии свободных рабочих мест;
- о реализации государственной программы приватизации;
- о ликвидации юридического лица;
- для которой определены ограничения по установлению режима коммерческой тайны в соответствии с федеральными законами и принятыми в целях их реализации подзаконными актами.

Основными субъектами права на коммерческую тайну являются обладатели коммерческой тайны, их правопреемники.

Обладатели коммерческой тайны - физические (независимо от гражданства) и юридические (коммерческие и некоммерческие организации) лица, занимающиеся предпринимательской деятельностью и имеющие монопольное право на информацию, составляющую для них коммерческую тайну.

Правопреемники - физические и юридические лица, которым в силу служебного положения, по договору или на ином законном основании (в том числе по наследству) известна информация, составляющая коммерческую тайну другого лица.

Перечень сведений, относящихся к КТ и носящий рекомендательный характер, может быть сгруппирован по тематическому принципу. Сведения, включенные в данный перечень, могут быть КТ только с учетом особенностей конкретного предприятия (организации).

1. **Сведения о финансовой деятельности –** прибыль, кредиты, товарооборот; финансовые отчеты и прогнозы; коммерческие замыслы; фонд заработной платы; стоимость основных и оборотных средств; кредитные условия платежа; банковские счета; плановые и отчетные калькуляции.

2. **Информация о рынке** - цены, скидки, условия договоров, спецификация продукции, объем, история, тенденции производства и прогноз для конкретного продукта; рыночная политика и планирование; маркетинг и стратегия цен; отношения с потребителем и репутация; численность и размещения торговых агентов; каналы и методы сбыта; политика сбыта; программа рекламы.

3. **Сведения о производстве продукции** - сведения о техническом уровне, технико-экономических характеристиках разрабатываемых изделий; сведения о планируемых сроках создания разрабатываемых изделий; сведения о применяемых и перспективных технологиях, технологических процессах, приемах и оборудовании; сведения о модификации и модернизации ранее известных технологий, процессов, оборудования; производственные мощности; состояние основных и оборотных фондов; организация производства; размещение и размер производственных помещений и складов; перспективные планы развития производства; технические спецификации существующей и перспективной продукции; схемы и чертежи новых разработок; оценка качества и эффективности.

4. **Сведения о научных разработках** - новые технологические методы, новые технические, технологические и физические принципы;

программы НИР; новые алгоритмы; оригинальные программы.

5. **Сведения о материально-техническом обеспечении** - сведения о составе торговых клиентов, представителей и посредников; потребности в сырье, материалах, комплектующих узлах и деталях, источники удовлетворения этих потребностей; транспортные и энергетические потребности.

6. **Сведения о персонале предприятия** - численность персонала предприятия; определение лиц, принимающих решения.

7. **Сведения о принципах управления предприятием** - сведения о применяемых и перспективных методах управления производством;

сведения о. фактах ведения переговоров, предметах и целей совещаний и заседаний

органов управления; сведения о планах предприятия по расширению производства; условия продажи и слияния фирм.

8. Прочие сведения - важные элементы системы безопасности, кодов и процедур доступа, принципы организации защиты коммерческой тайны.

Банковская тайна - защищаемые банками и иными кредитными организациями сведения о банковских операциях по счетам и сделкам в интересах клиентов, счетах и вкладах своих клиентов и корреспондентов, а также сведения о клиентах и корреспондентах, разглашение которых может нарушить право последних на неприкосновенность частной жизни.

К основным объектам банковской тайны относятся следующие:

1.Тайна банковского счета - сведения о счетах клиентов и корреспондентов и действиях с ними в кредитной организации;

2.Тайна операций по банковскому счету - сведения о принятии и зачислении поступающих на счет клиента денежных средств, о выполнении его распоряжений по перечислению и выдаче соответствующих сумм со счета;

3.Тайна банковского вклада - сведения обо всех видах вкладов клиента в кредитной организации.

4. Тайца частной жизни клиента.

Служебная тайна - защищаемая по закону конфиденциальная информация, ставшая известной в государственных органах и органах местного самоуправления только на законных основаниях и в силу исполнения, их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости.

Служебная тайна является видом конфиденциальной информации, и право на служебную тайну выступает самостоятельным объектом права. Для осуществления ее правовой охраны и защиты необходим специальный Федеральный закон «О служебной тайне».

Информация может считаться служебной тайной, если она отвечает следующим требованиям (критериям охраноспособности права):

- ✓ отнесена федеральным законом к служебной информации о деятельности государственных органов, доступ к которой ограничен по закону или в силу служебной необходимости (собственная служебная тайна);
- ✓ является охраноспособной конфиденциальной информацией ("чужой тайной") другого лица (коммерческая тайна, банковская тайна, тайна частной жизни, профессиональная тайна);

Профессиональная тайна - защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной или муниципальной службой, распространение которой может нанести ущерб правам и законным интересам другого лица (доверителя), доверившего эти сведения, и не являющаяся государственной или коммерческой тайной.

Информация может считаться профессиональной тайной, если она отвечает следующим требованиям (критериям охраноспособности права):

-доверена или стала известна лицу лишь в силу исполнения им своих профессиональных обязанностей;

- запрет на распространение доверенной или ставшей известной информации, которое может нанести ущерб правам и законным интересам доверителя, установлен федеральным законом;

- информация не относится к сведениям, составляющим государственную и коммерческую тайну.

В соответствии с этими критериями можно выделить следующие объекты профессиональной тайны:

1. Врачебная тайна
2. Тайна связи.
3. Нотариальная тайна.
4. Адвокатская тайна.
5. Тайна усыновления.
6. Тайна страхования.

Персональные данные

1) Персональные данные – любая информация, относящаяся к физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

2) Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

В случаях, предусмотренных Федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Письменное согласие субъекта персональных данных на обработку своих персональных данных должно включать в себя:

1) Фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) Наименование (фамилия, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;

3) Цель обработки персональных данных;

4) Перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

5) Перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способом обработки персональных данных;

6) Срок, в течение которого действует согласие, а также порядок его отказа.

Контрольные вопросы по теме 1

1. Назовите особенности современного информационного общества.
2. Какие элементы информационной инфраструктуры Вы знаете?
3. Что понимается под угрозой безопасности информации?
4. Дайте определение информационной безопасности на предприятии.
5. Назовите объекты информационной безопасности на предприятии.
6. Какие обеспечивающие подсистемы включает система защиты информации?
7. Назовите особенности экономической информации.
8. В чем отличия понятий информационный ресурс, продукт и услуга?
9. Как определяется цена информационного продукта?
10. Что такое конфиденциальность, целостность и доступность информации?
11. Какая информация компании не может быть отнесена к коммерческой тайне?

12. Что такое персональные данные?

Тесты к теме №1

1. Информационная война – это…

А. злословие в адрес другого человека;

Б. информационное противоборство с целью нанесения ущерба важным структурам противника, подрыв его политической и социальной систем, а также дестабилизации общества и государства противника;

В. акт применения информационного оружия.

2. Информационная безопасность – это…

А. невозможность нанесения вреда свойствам объектам безопасности, обуславливаемым информацией и информационной инфраструктурой (защищенность от угроз);

Б. предотвращение зла наносимого государственным структурам;

В. проведение природоохранных мероприятий.

3. К понятию информационной безопасности НЕ относятся:

А. природоохранные мероприятия;

Б. надежность работы компьютера;

В. сохранность ценных данных.

4. К объектам информационной безопасности на предприятии НЕ относятся:

А. информационные ресурсы;

Б. средства вычислительной и организационной техники;

В. Конституция России.

5. Обеспечение безопасности информации – это…

А. одноразовое мероприятие;

Б. комплексное использование всего арсенала имеющихся средств защиты;

В. разработка каждой службой плановых мер по защите информации.

6. Лингвистическое обеспечение информационной безопасности – это?

А. реализация защиты информации структурными единицами, такими как: служба безопасности, служба режима и т.д.;

Б. нормы и регламенты деятельности органов, служб, средств, реализующих функции защиты информации;

В. совокупность специальных языковых средств общения специалистов и пользователей в сфере защиты информации.

7. Эргономическое обеспечение информационной безопасности – это?

А. антивирусные программы;

Б. совокупность средств, обеспечивающих удобства работы пользователей аппаратных средств защиты информации;

В. комплекс математических методов, связанных с оценкой опасности технических средств.

8.Информационное обеспечение информационной безопасности – это?

А. совокупность специальных языковых средств общения специалистов и пользователей в сфере защиты информации;

Б. антивирусные программы;

В. документированные сведения, лежащие в основе решения задач, обеспечивающих функционирование системы.

9. Организационное обеспечение информационной безопасности – это?

А. реализация защиты информации структурными единицами, такими как: служба безопасности, служба режима и т.д.;

Б. совокупность средств;

В. нормативные документы по ИБ, требование которых являются обязательными в рамках сферы действия каждого подразделения.

10. К основным угрозам информационной безопасности НЕ относятся:

А. раскрытие конфиденциальной информации;

Б. нарушение принципов экономической безопасности;

В. отказ от обслуживания.

11. Информационное оружие – это?

А. комплекс технических средств, методов и технологий, направленных против управленческих систем;

Б. нормативно-правовая база по информационной безопасности;

В. комплекс индивидуального и общественного сознания.

12. Правовое обеспечение информационной безопасности – это..?

А. нормативные документы по ИБ, требования которых являются обязательными в рамках сферы действия каждого подразделения;

Б. документированные сведения, лежащие в основе решения задач, обеспечивающих функционирование системы;

В. широкое использование технических средств защиты информации.

13.Экономическая информация является товаром?

А. да;

Б. нет;

В. кроме конфиденциальных сведений.

14. К числу особенностей информации как товара НЕ относятся:

А. сохраняемость;

Б. несамостоятельность;

В. самостоятельность.

15 .Информация может составлять коммерческую тайну, если:

А. к ней нет свободного доступа на законном основании;

Б. содержится в учредительных документах;

В. содержится в бухгалтерском балансах.

16. Не являются коммерческой тайной?

А. сведения, содержащиеся в документах, дающие право заниматься предпринимательской деятельностью;

Б. сведения о научных разработках;

В. сведения о персонале предприятия.

17. Конфиденциальность компьютерной информацией – это?

А. предотвращение проникновения компьютерных вирусов в память ПЭВМ;

Б. свойство информации быть известной только допущенным и прошедшим проверку (авторизацию) субъектам системы;

В. безопасное программное обеспечение.

18. Банковская тайна – это..?

А. информация о банковском счете, вкладе, операциях по счету, о клиентах банка;

Б. информация о сотрудниках банка;

В. информация о режиме работы банка.

19. Объектами профессиональной тайны НЕ являются:

А. тайна страхования;

Б. врачебная тайна;

В. бухгалтерский баланс.