ЛЕКЦИЯ №2 **Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования.**

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

Учебные вопросы:

1. Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования
2. ГОСТ Р 50739-95 «Защита от несанкционированного доступа к информации. Общие технические требования»
3. Типовая инструкция по эксплуатации телекоммуникационного оборудования

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

В рамках данной лекции будет проведен обзор существующей отечественной и зарубежной нормативной правовой базы в области информационной безопасности (ИБ) сетевого оборудования, с целью определения конкретных требований к ТКО, направленных на обеспечение его защиты от компьютерных атак и иных противоправных воздействий, диагностики технического состояния и уровня его защищенности, а также аудита всех действия оператора.

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

Нормативную правовую базу, в области информационной безопасности сетей и сетевого оборудования можно разделить на :

– Постановления Правительства Российской Федерации;

– Федеральные законы Российской Федерации;

– ведомственные приказы (ФСБ России, ФСТЭК России и т.д.)

– государственные стандарты Российской Федерации (ГОСТ Р);

– государственные военные стандарты Российской Федерации (ГОСТ РВ);

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

– стандарты СССР (ГОСТ, ГОСТ В), не отменённые на настоящий момент;

– рекомендации сектора стандартизации электросвязи Международного союза электросвязи (International Telecommunication Union – Telecommunication sector, ITU-T);

– стандарты IEEE (Institute of Electrical and Electronics Engineers, Институт инженеров по электротехнике и электронике), прежде всего – группа стандартов IEEE 802, касающихся локальных вычислительных сетей (LAN) и сетей мегаполисов (MAN).

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

Следует отметить, что в Российской Федерации отсутствуют государственные стандарты, которые регламентировали бы напрямую вопросы информационной безопасности ТКО. В тоже время, можно отметить ГОСТ Р 50739-95 «Защита от несанкционированного доступа к информации. Общие технические требования», в котором отсутствует понятие ТКО, но, учитывая современные функциональные возможности и принципы построения ТКО, предлагаемые ГОСТ Р 50739-95 требования к СВТ могут предъявляться и к ТКО.

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

Среди ведомственных нормативных требований к ТКО следует, прежде всего, выделить требования ФСБ России и ФСТЭК России.

На настоящий момент ФСТЭК России по требованиям к межсетевым экранам сертифицировано несколько десятков моделей маршрутизаторов и коммутаторов Cisco.

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

Для большинства маршрутизаторов и коммутаторов Cisco, сертифицированных ФСТЭК России по требованиям к межсетевым экранам, имеющийся в них функционал межсетевого экранирования не является значимым для конечного пользователя, а требования к межсетевым экранам используются как наиболее применимые для маршрутизаторов и коммутаторов (за неимением в ФСТЭК России полноценных требований к телекоммуникационному оборудованию).

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

В связи с отсутствием в ФСТЭК России специализированных требований к ТКО, существует практика сертификации отдельных моделей телекоммуникационного оборудования по требованиям к средствам вычислительной техники. Например, в связи с отсутствием в ФСТЭК России специализированных требований к автоматическим телефонным станциям (АТС), АТС «HUAWEI C&C08» сертифицирована по требованиям Руководящего документа Гостехкомиссии России (предшественник ФСТЭК России) «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости. Показатели защищённости от несанкционированного доступа к информации», как СВТ 6 класса защищённости от несанкционированного доступа.

Кроме того, в ФСТЭК России существует практика сертификации ТКО на соответствие требованиям технических условий (например – Cisco Catalyst 3750, Cisco WS-6506-EXL-FWM-K9), то есть в этих случаях нормативным документом выступают ТУ разработчиков соответствующего оборудования, а ФСТЭК России при сертификации только подтверждает соответствие фактических характеристик ТКО заявленным в документации.

Также, необходимо выделить Руководящий документ Гостехкомиссии России **Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей** (далее – НДВ). Данный Руководящий документ регламентирует порядок исследований ПО (в том числе, ПО ТКО и СУ ТКО) на отсутствие НДВ, предъявляет требования к исходным текстам ПО и его документации.

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

Далее будет проведён анализ нормативных документов различных организаций и ведомств, регламентирующих вопросы информационной безопасности сетей связи. При проведении анализа наибольшее внимание уделялось разделам нормативных документов, в которых приводились механизмы защиты и средства диагностического исследования ТКО.

Кроме того, проводился поиск мер, направленных на повышение уровня защищённости ТКО, включая требования к создаваемым образцам и уже применяемым решениям, комплексным подходам защиты сетей связи общего, корпоративного и специального назначения, а также исследовались требования к функциональным возможностям оборудования, с точки зрения противодействия потенциальным компьютерным атакам.

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

Нормативный правовой акт	Содержание нормативного правового акта в части безопасности сетей
Постановление Правительства Российской Федерации «О присоединении информационных систем организаций к инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»	Статья 11. Операторы информационных систем органов и организаций, а также оператор информационных систем, входящих в состав инфраструктуры взаимодействия, при организации взаимодействия информационных систем между собой, а также с элементами инфраструктуры взаимодействия обязаны: а) обеспечивать защиту передаваемых сведений от неправомерного доступа, уничтожения, модификации, блокирования, копирования, распространения, иных неправомерных действий с момента поступления этих сведений в свою информационную систему и до момента их поступления в информационные системы, эксплуатируемые иными операторами; б) обеспечивать соблюдение конфиденциальности информации ограниченного доступа в соответствии с требованиями законодательства Российской Федерации.

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

Нормативный правовой акт	Содержание нормативного правового акта в части безопасности сетей
Федеральный Закон Российской Федерации № 149-ФЗ «Об информации, информационных технологиях и о защите информации»	Статья 16. Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации; недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

Нормативный правовой акт	Содержание нормативного правового акта в части безопасности сетей
Федеральный Закон Российской Федерации № 152-ФЗ «О персональных данных»	Статья 19, п. 1. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

Нормативный правовой акт	Содержание нормативного правового акта в части безопасности сетей
Федеральный закон Российской Федерации от 21 июля 2011 г. № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса»	Статья 11, п. 1. В целях обеспечения безопасности объектов топливно-энергетического комплекса субъекты топливно-энергетического комплекса создают на этих объектах системы защиты информации и информационно-телекоммуникационных сетей от неправомерных доступа, уничтожения, модифицирования, блокирования информации и иных неправомерных действий и обеспечивают функционирование таких систем. Создание таких систем предусматривает планирование и реализацию комплекса технических и организационных мер, обеспечивающих в том числе антитеррористическую защищённость объектов топливно-энергетического комплекса.

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

Нормативный правовой акт	Содержание нормативного правового акта в части безопасности сетей
Совместный Приказ ФСБ России № 416, ФСТЭК России № 489 от 31.08.2010 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»	В информационных системах общего пользования должны быть обеспечены: поддержание целостности и доступности информации; предупреждение возможных неблагоприятных последствий нарушения порядка доступа к информации; проведение мероприятий, направленных на предотвращение неправомерных действий в отношении информации.

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

Нормативный правовой акт	Содержание нормативного правового акта в части безопасности сетей
Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»	Раздел 2. Состав и содержание мер по обеспечению безопасности персональных данных Пп. 8.5. Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них. Пп. 8.14 Меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

Нормативный правовой акт	Содержание нормативного правового акта в части безопасности сетей
Приказ ФСТЭК № 17 «Об утверждении Требований по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»	Пп. 18.2. В ходе выявления инцидентов и реагирования на них осуществляются обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов. Пп. 20.7. Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) информацию в целях её добывания, уничтожения, искажения и блокирования действия.

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

Нормативный правовой акт	Содержание нормативного правового акта в части безопасности сетей
Руководящий документ РД-21-02-2006 «Типовая инструкция о защите информации в автоматизированных средствах центрального аппарата, территориальных органов и организаций федеральной службы по экологическому, технологическому и атомному надзору» (Ростехнадзор России)	Пп. 3.7. Должностные лица, отвечающие за безопасность информации и входящие в систему защиты информации в компьютерных и телекоммуникационных сетях Федеральной службы по экологическому, технологическому и атомному надзору, контролируют в пределах своей компетенции состояние защиты информации с целью своевременного выявления и предотвращения утечки информации по техническим каналам, несанкционированного доступа к ней, преднамеренных программно-технических воздействий на информацию и оценки её защищённости.

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

Нормативный правовой акт	Содержание нормативного правового акта в части безопасности сетей
Положение ЦБ РФ от 9 июня 2012 г. № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»	Пп. 2.7.1. Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают: использование технических средств защиты информации, предназначенных для выявления вредоносного кода и для предотвращения воздействия вредоносного кода на объекты информационной инфраструктуры (далее – технические средства защиты информации от воздействия вредоносного кода), на средствах вычислительной техники, включая банкоматы и платежные терминалы. Пп. 2.13.2. Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для выявления инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств;

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

Нормативный правовой акт	Содержание нормативного правового акта в части безопасности сетей
Стандарт Банка России СТО БР ИББС–1.0–2014. «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения»	Пп. 7.4.4. В организации банковской сферы РФ должны быть определены, выполняться, регистрироваться и контролироваться правила и процедуры мониторинга ИБ, анализа и хранения данных о действиях и операциях, позволяющие выявлять неправомерные или подозрительные операции и транзакции, для чего, среди прочего, следует: определить действия и операции, подлежащие регистрации; определить состав и содержание данных о действиях и операциях, подлежащих регистрации, сроки их хранения обеспечить резервирование необходимого объема памяти для записи данных; обеспечить реагирование на сбои при регистрации действий и операций, в том числе аппаратные и программные ошибки, сбои в технических средствах сбора данных; обеспечить генерацию временных меток для регистрируемых действий и операций и синхронизацию системного времени на технических средствах, используемых для целей мониторинга ИБ, анализа и хранения данных.

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

Нормативный правовой акт	Содержание нормативного правового акта в части безопасности сетей
Стандарт Банка России СТО БР ИББС–1.0–2014. «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения»	В организации БС РФ должно быть реализовано ведение журналов действия и операций автоматизированных рабочих мест, серверного и сетевого оборудования, межсетевых экранов с целью их использования при реагировании на инциденты ИБ. Для проведения процедур мониторинга ИБ и анализа данных о действиях и операциях следует использовать специализированные программные и (или) технические средства. Процедуры мониторинга ИБ и анализа данных о действиях и операциях должны использовать зафиксированные критерии выявления неправомерных или подозрительных действий и операций. Указанные процедуры мониторинга ИБ и анализа должны применяться на регулярной основе.

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

Нормативный правовой акт	Содержание нормативного правового акта в части безопасности сетей
Стандарт Банка России СТО БР ИББС–1.0–2014. «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения»	Пп. 8.10. Требования к организации обнаружения и реагирования на инциденты информационной безопасности Пп. 8.10.1. Должны быть определены, выполняться, регистрироваться и контролироваться: процедуры обработки инцидентов, включающие: процедуры обнаружения инцидентов ИБ; процедуры информирования об инцидентах, в том числе информирования службы ИБ; процедуры классификации инцидентов и оценки ущерба, нанесенного инцидентом ИБ; процедуры реагирования на инцидент; процедуры анализа причин инцидентов ИБ и оценки результатов реагирования на инциденты ИБ (при необходимости с участием внешних экспертов в области ИБ).

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

Нормативный правовой акт	Содержание нормативного правового акта в части безопасности сетей
Стандарт Банка России СТО БР ИББС–1.0–2014. «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения»	Пп. 8.10.2. Должны быть определены, выполняться, регистрироваться и контролироваться процедуры хранения и распространения информации об инцидентах ИБ, практиках анализа инцидентов ИБ и результатах реагирования на инциденты ИБ. Пп. 8.10.3. Должны быть определены, выполняться, регистрироваться и контролироваться действия работников организации БС РФ при обнаружении нетипичных событий, связанных с ИБ, и информировании о данных событиях. Работники организации должны быть осведомлены об указанных порядках. Пп. 8.10.4. Процедуры расследования инцидентов ИБ должны учитывать законодательство РФ, положения нормативных актов Банка России, а также внутренних документов организации БС РФ в области ИБ. Пп. 8.10.5. В организациях БС РФ должны приниматься, фиксироваться и выполняться решения по всем выявленным инцидентам ИБ. Пп. 8.10.6. В организации БС РФ должны быть определены роли по обнаружению, классификации, реагированию, анализу.

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

Нормативный правовой акт	Содержание нормативного правового акта в части безопасности сетей
Приказ Министерства информационных технологий и связи РФ от 9 января 2008 г. № 1 «Об утверждении требований по защите сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации»	П. 7. Для защиты от несанкционированного доступа к программным средствам узлов связи сетей фиксированной телефонной связи, сетей подвижной радиосвязи, сетей подвижной радиотелефонной связи, сетей подвижной спутниковой радиосвязи, сетей передачи данных, сетей телеграфной связи операторы связи обеспечивают принятие мер, исключающих возможность доступа к сетям связи лиц, не имеющих на это права, или абонентов и пользователей, нарушающих установленный оператором связи порядок доступа к сети связи.

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

Нормативный правовой акт	Содержание нормативного правового акта в части безопасности сетей
Приказ Минкомсвязи России от 27.12.2010 № 190 «Технические требования к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия»	П. 10. При создании и эксплуатации информационной системы общего пользования осуществляется регистрация действий обслуживающего персонала и аномальной активности пользователей; П. 12. Операторы информационной системы общего пользования обязаны обеспечивать постоянный контроль обеспечения защищённости информационной системы общего пользования от неправомерных действий.

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

Нормативный правовой акт	Содержание нормативного правового акта в части безопасности сетей
Приказ Министерства информационных технологий и связи Российской Федерации от 15 мая 2007 г. № 55 «Об утверждении правил применения оборудования автоматизированных систем управления и мониторинга сетей электросвязи. Часть 1. Правила применения оборудования автоматизированных систем управления и мониторинга средств связи, выполняющих функции систем коммутации каналов правила применения оборудования автоматизированных систем управления и мониторинга сетей электросвязи»	Оборудование автоматизированных систем управления и мониторинга средств связи, выполняющих функции систем коммутации каналов, обеспечивает выдачу сообщений о попытках несанкционированного доступа к системам коммутации каналов.

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

Нормативный правовой акт	Содержание нормативного правового акта в части безопасности сетей
Методические рекомендации по формированию требований к обеспечению информационной безопасности информационных систем и ресурсов города Москвы	Требования к подсистеме обнаружения несанкционированной активности: осуществлять обнаружение несанкционированной активности на сетевом, системном и прикладном уровнях; обнаружение атак на информационные ресурсы на основе сравнения текущего состояния систем (сетевой активности, системных и прикладных журналов аудита и др.) с сигнатурами атак; возможность прекращения несанкционированной активности; регистрировать зафиксированные несанкционированные действия, в том числе дата и время события, тип события, идентификатор субъекта, приоритет события;

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

Нормативный правовой акт	Содержание нормативного правового акта в части безопасности сетей
Методические рекомендации по формированию требований к обеспечению информационной безопасности информационных систем и ресурсов города Москвы	удаленное обновление базы данных сигнатур атак; обеспечение доступа к базе данных зафиксированных событий, включая возможность поиска, сортировки, упорядочения записей протоколов, основанный на заданных критериях; обеспечение уведомления администратора о фактах несанкционированной сетевой активности (локально и удаленно); разграничение прав доступа операторов и администраторов к различным компонентам системы.

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

Нормативный правовой акт	Содержание нормативного правового акта в части безопасности сетей
Совместный приказ от 2 марта 2009 года Федеральной миграционной службы № 39, Министерства внутренних дел Российской Федерации № 179, Министерства иностранных дел Российской Федерации № 2619 … № ММ-7-6/100 «О типовом соглашении об информационном обмене сведениями в государственной информационной системе миграционного учёта»	Участники информационного обмена обязуются: соблюдать требования информационной безопасности информационной системы, принимать меры по предотвращению несанкционированного доступа к сведениям и средствам вычислительной техники информационной системы.

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

Нормативный правовой акт	Содержание нормативного правового акта в части безопасности сетей
Приказ ФССП России от 12.05.2012 № 248 «Об утверждении Порядка создания и ведения банка данных в исполнительном производстве Федеральной службы судебных приставов»	Пп. 8.4. Подразделение, ответственное за обеспечение информационной безопасности в центральном аппарате Федеральной службы судебных приставов (ФССП) России (в территориальном органе ФССП России), осуществляет выявление и учёт фактов несанкционированного доступа к банку данных, а также принятие мер по проверке и расследованию инцидентов безопасности информации, в том числе с использованием программных, программно-аппаратных и технических средств.

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

Нормативный правовой акт	Содержание нормативного правового акта в части безопасности сетей
Приказ Федеральной службы по финансовым рынкам от 3 июля 2012 г. № 12-53/пз-н «Об утверждении требований к некоторым внутренним документам центрального депозита»	П. 3. При взаимодействии информационных систем центрального депозитария с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования) правила защиты информации центрального депозитария должны также предусматривать: 1) использование средств межсетевого экранирования для управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы; 2) методы обнаружения вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению информационной безопасности; 3) методы анализа защищённости информационных систем центрального депозитария посредством специализированных программных средств (сканеров безопасности); 4) описание способов защиты информации при её передаче по каналам связи.

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

Нормативный правовой акт	Содержание нормативного правового акта в части безопасности сетей
Приказ Министерства здравоохранения и социального развития Российской Федерации от 3 мая 2012 года «Методические рекомендации по оснащению медицинских учреждений компьютерным оборудованием и программным обеспечением для регионального уровня единой государственной информационной системы в сфере здравоохранения, а также функциональные требования к ним»	В состав регионального программно-технического комплекса должен быть включен сервер информационной безопасности. Сервер информационной безопасности является неотъемлемой частью системы и должен обеспечивать безопасность телекоммуникационных сетей предприятия, интегрируясь в существующую сетевую инфраструктуру.

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

Нормативный правовой акт	Содержание нормативного правового акта в части безопасности сетей
Рекомендации Международного Союза Электросвязи № Е. 408 «Требования к безопасности сетей Электросвязи»	П. 6.3. Услуги безопасности: - аутентификация пользователя; - аутентификация источника данных; - управление доступом к ассоциации административного управления; - управление доступом к извещению административного управления; - управление доступом к управляемому ресурсу; - аварийный сигнал безопасности, аудиторский журнал и восстановление; - выборочная целостность поля; - целостность соединения с восстановлением; - целостность соединения без восстановления; - выборочная конфиденциальность поля; - конфиденциальность соединения/связи без соединения; - конфиденциальность потока трафика; - защита от непризнания участия: доказательство передачи; - защита от непризнания участия: доказательство доставки.

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

Нормативный правовой акт	Содержание нормативного правового акта в части безопасности сетей
Стандарт инженеров по электротехнике и электронике IEEE 802.10 «Сетевая безопасность»	Пп. 2К.3 Требования по безопасности - параметры безопасности должны быть зафиксированы в разрабатываемом «Перечне информации, подлежащей защите». Установление уровня защиты информации в системе и определение параметров определяется на месте эксплуатации. - сформированный «Перечень информации, подлежащей защите» должен разрабатываться для каждого оборудования, входящего в состав системы. Значение параметров должно быть установлено с соответствии с требованиями нормативных документов для по безопасности. Значения параметров должны быть четко определены и могут содержать только одно значение.

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

Нормативный правовой акт	Содержание нормативного правового акта в части безопасности сетей
Стандарт инженеров по электротехнике и электронике IEEE 802.10 «Сетевая безопасность»	- попытка выполнить мероприятия, противоречащие установленным правилам по безопасности, должны быть зафиксированы в электронном журнале; -должна быть реализована функция уведомления пользователя об ошибке. - системный администратор обеспечивает настройку оборудования, определяет параметры и события безопасности, требующие контроля. В результате процесса контроля должен быть сформировано уведомление пользователю (оператору), основанное на утвержденной политике безопасности. - если фиксируемая информация по безопасности не может поместиться в электронный журнал, то должно быть выдано сообщение об ошибке. Также, должна быть реализована возможность передачи уведомления об ошибке пользователю.

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

Нормативный правовой акт	Содержание нормативного правового акта в части безопасности сетей
Стандарт инженеров по электротехнике и электронике IEEE 802.11i «Информационная безопасность беспроводных технологий»	Пп. 5.4.3.1 Запрещается повторное использование одних и тех же ключей шифрования. Для установления сеанса связи необходимо создание специального сеансового криптографического ключа для шифрования всей передаваемой информации. Пп. 5.4.2.2. Авторизация. Вместо механизма локальной авторизации необходимо применение схемы аутентификации, разработанной в рамках стандарта IEEE 802.1X. Данная схема предусматривает прохождение процесса авторизации и принятия решения о предоставлении доступа пользователя к сети (оборудованию) на выделенном сервере аутентификации.

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

Нормативный правовой акт	Содержание нормативного правового акта в части безопасности сетей
Стандарт инженеров по электротехнике и электронике IEEE 802.11i «Информационная безопасность беспроводных технологий»	Пп. 8.3. Протоколы конфиденциальной передачи данных. Вместо криптографического алгоритма WEP должен применяться криптографический протокол CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), который использует для зашифрования/расшифрования информации - алгоритм AES (Advanced Encryption Standard). Пп. 8.3.2. В процессе перехода с алгоритма WEP на протокол CCMP необходимо применение протокола TKIP (Temporal Key Integrity Protocol, протокол обеспечения временной целостности криптографических ключей

Следует подробнее остановиться на анализе упомянутого выше ГОСТ Р 50739-95 «Защита от несанкционированного доступа к информации. Общие технические требования».

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

В ГОСТ Р 50739-95 можно выделить следующие группы требований по защите информации, применимые для современных образцов ТКО:

1. Требования к системе разграничения доступа, предусматривающие поддержку непротиворечивых, однозначно определенных правил разграничения доступа

(п. 5.1. Требования к разграничению доступа)

а) дискретизационный принцип контроля доступа;

б) идентификация и аутентификация;

в) сопоставление пользователя с устройством.

ЛЕКЦИЯ №2 Существующая отечественная и зарубежная нормативно-правовая база в области информационной безопасности сетевого оборудования

1.1. Для реализации дискретизационного принципа контроля доступа (комплекс средств защиты) КСЗ должен контролировать доступ именованных субъектов (**пользователей**) к именованным объектам (например, **файлам**, программам, томам).

1.2. Для каждой пары (субъект - объект) в должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (например, читать, писать), т.е. тех типов доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу СВТ (объекту).

1.3. Право изменять правила разграничения доступа (ПРД) должно быть предоставлено выделенным субъектам (например, администрации, службе безопасности).

1.4. Должны быть предусмотрены средства управления, ограничивающие распространение прав на доступ.

1.5. Субъект может читать объект, если уровень иерархической классификации в классификационном уровне субъекта не меньше, чем уровень иерархической классификации в классификационном уровне субъекта, и неиерархические категории в классификационном уровне субъекта включают в себя все неиерархические категории в классификационном уровне объекта:

1.6. Субъект осуществляет запись в объект, если классификационный уровень субъекта в иерархической классификации не больше, чем классификационный уровень объекта в иерархической классификации, и все неиерархические категории в классификационном уровне субъекта включены в неиерархические категории в классификационном уровне объекта.

1.7. КСЗ должен обеспечивать идентификацию субъектов при запросах на доступ, должен проверять подлинность идентификатора субъекта (осуществлять аутентификацию). КСЗ должен располагать необходимыми данными для идентификации и аутентификации и препятствовать доступу к защищаемым ресурсам неидентифицированных субъектов или субъектов, чья подлинность при аутентификации не подтвердилась.

Требования к системе учёта, предусматривающие поддержку регистрации событий, имеющих отношение к информационной безопасности;

2.1. КСЗ должен осуществлять регистрацию следующих событий:

а) использование идентификационного и аутентификационного механизма;

б) запрос на доступ к защищаемому ресурсу (например, открытие файла, запуск программы);

в) действия, связанные с изменением ПРД.

Для каждого из этих событий должна быть зарегистрирована следующая информация:

- дата и время;
- субъект, осуществляющий регистрируемое действие;
- тип события (если регистрируется запрос на доступ, то отмечают объект и тип доступа);
- успешно ли осуществилось событие (обслужен запрос на доступ или нет).

3. Требования к гарантиям, определяющие наличие программных и аппаратных механизмов обеспечивающих выполнение требований к системам разграничения доступа и учёта.

3.1. Требования к гарантиям определяют следующие показатели защищенности, которые должны поддерживаться СВТ:

а) контроль модификации;

б) контроль дистрибуции;

в) тестирование.

3.2. Процедуры восстановления после сбоев и отказов оборудования должны обеспечивать полное восстановление свойств КСЗ.

3.4. В СВТ должны быть предусмотрены средства периодического контроля за целостностью программной и информационной части КСЗ.

На основе указанных выше документов разрабатывается типовая инструкция по эксплуатации телекоммуникационного оборудования, в которую, обычно, входят следующие разделы.

- **общие требования к ТКО и системе управления ТКО (СУ ТКО)** – определяющие состав программно-аппаратных средств, требования к составу и квалификации обслуживающего персонала;

- **требования к специализированным средствам защиты и специальные требования к ТКО** – определяющие основные свойства применяемых специальных средств защиты (средства криптографической защиты информации (СКЗИ), межсетевые экраны, средства обнаружения компьютерных атак);

- **требования по размещению ТКО и СУ ТКО** – определяющие основные условия и особенности монтажа и установки оборудования, его электропитания и защитного заземления, а также требования к помещению в котором оно размещается;

- **требования по сопряжению ТКО с оборудованием ЛВС и внешних сетей** – определяющие классы применяемых устройств межсетевого экранирования и устройств обнаружения компьютерных атак;

- **требования по защите каналов удаленного управления ТКО** – определяющие необходимость использования для защиты канала управления сертифицированных СКЗИ прошедших исследования в составе с телекоммуникационным оборудованием;

- **требования по эксплуатации** – определяющие количество и состав рабочих мест СУ ТКО, параметры их настройки, порядок ввода в эксплуатацию, политику назначения и смены паролей операторов, требования по проверке ПЭВМ СУ ТКО, а также требования по проверке отключения неразрешенных сервисов и функций;

- **организационно-технические требования** – определяющие порядок допуска оборудования к эксплуатации, регламенты осуществления проверок целостности ПО, порядок действий в случае выявленных нарушений;

- **требования по проведению ремонтно-профилактических работ** – определяющие требования к лицам допущенным к проведению указанных работ, действия обслуживающего персонала после их проведения, а также порядок передачи компонентов ТКО для устранения неисправностей разработчику оборудования;

- **требования по организации и ведению регистрационных журналов** – определяющие состав, порядок доступа, а также сроки учета и хранения электронных журналов работы оборудования и действий обслуживающего персонала, порядок действий в случае выявления нарушений;