РУКОВОДЯЩИЕ УКАЗАНИЯ ПО КИБЕРБЕЗОПАСНОСТИ В КОНТЕКСТЕ ISO 27032

***Марков Алексей Сергеевич**, кандидат технических наук, старший научный сотрудник, CISSP,*
***Цирлов Валентин Леонидович**, кандидат технических наук, CISSP*

Рассмотрен новый стандарт по кибербезопасности ISO/IEC 27032. Проведен анализ понятий, тезауруса и онтологии кибербезопасности в сравнении с категориями информационной безопасности. Рассмотрены руководящие принципы и организационно-технические меры кибербезопасности. Дано краткое описание методов повышения готовности. Отмечены вопросы гармонизации стандарта в рамках российской нормативной базы. Отмечены ограничения, недостатки и область применения стандарта в России.

***Ключевые слова**: кибербезопасность, киберпространство, киберугрозы, кибер-риски, стейкхолдеры, ИСО 27032, ГОСТ 27005, ГОСТ 27000, меры кибербезопасности, методы и средства обеспечения безопасности*

GUIDELINES FOR CYBERSECURITY IN THE CONTEXT OF ISO 27032

***Alexey Markov**, Ph.D., Associate Professor , CISSP*
***Valentin Tsirlov**, Ph.D., CISSP*

The new standard ISO/IEC 27032 on cybersecurity is considered. The concepts, ontologies, thesaurus of the cybersecurity in comparison with categories of information security are analyzed. The guidelines, organizational and technical measures of cibersecurity are discussed. A brief description of the methods to improve readiness is presented. The harmonization of standards in the framework of the Russian is shown. The limitations and prospects of the standard in the Russian are noted.

***Keywords**: cybersecurity, cyber security, cyberspace, cyber threats, cyber risks, stakeholders, ISO 27032, ISO 27000, cybersecurity measures, security techniques*

Введение

В рамках обсуждения концептуальных основ кибербезопасности страны остро стоит вопрос совершенствования соответствующего понятийного аппарата. В литературе сложился ряд направлений толкования определения «кибербезопасность», отражающего различные аспекты военной политики, международного права, критических информационных инфраструктур, информационно-коммуникационных технологий и компьютерных сетей [1-10]. При этом наблюдается смешение формулировок, данных в различных концептуальных и нормативных документах. Что касается последних, то наибольшее внимание уделяют цитированию нового международного стандарта ISO/IEC 27032:2012 Information technology - Security techniques - Guidelines for cybersecurity.

Следует указать, в нашей стране уже сложился ряд национальных стандартов 27000-серии, гармонизированный с международной базой. Рассмотрению положений стандарта ISO 27032 и его связи с российской нормативной базой посвящена данная статья.

Структура стандарта по кибербезопасности

Международный стандарт ISO 27032 выполнен в стиле риск-ориентированного подхода, хотя и отличается от национальных стандартов ГОСТ 27001 и ГОСТ 27005, привязанных к 4-процессной модели жизненного цикла [11,12]. Стандарт определяет активы киберпространства и заинтересованные стороны, угрозы, рекомендации и меры по обработке рисков, причем в качестве специфической меры выделены указания по координации действий и обмену информацией (рис.1).

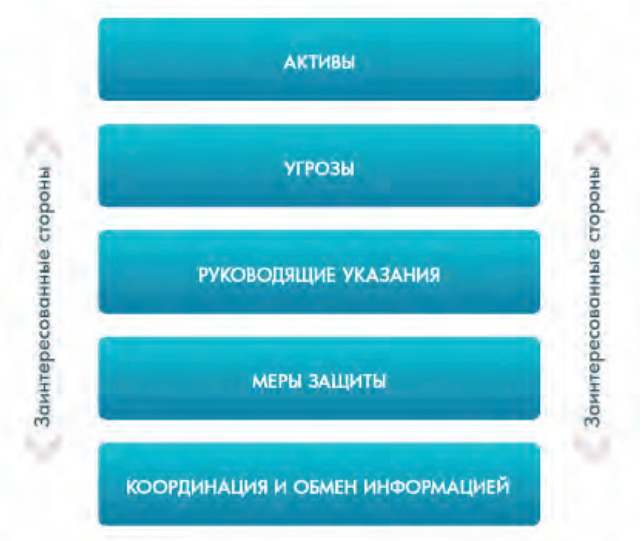


***Рис. 1**. Базовые блоки стандарта ISO 27032:2012*

Основные понятия кибербезопасности

По аналогии с классическим определением информационной безопасности в стандарте под *кибербезопасностью* фактически понимают свойство защищенности активов от угроз конфиденциальности, целостности, доступности, но в некоторых абстрактных рамках – киберпространстве.

Киберпространство формулируется как комплексная виртуальная среда (не имеющая физического воплощения), сформированная в результате действий людей, программ и сервисов в сети Интернет посредством соответствующих сетевых и коммуникационных технологий. Сущностями киберпространства могут быть виртуальные деньги, аватары, облака, виртуальные посольства, виртуальные преступления, виртуальные развлечения и т.д.

Что касается собственно обеспечения кибербезопасности, то в качестве приоритета выделена координация взаимодействия между организациями, формирующими киберпространство, самостоятельные действия которых не обеспечивают эффективную защиту от киберугроз.

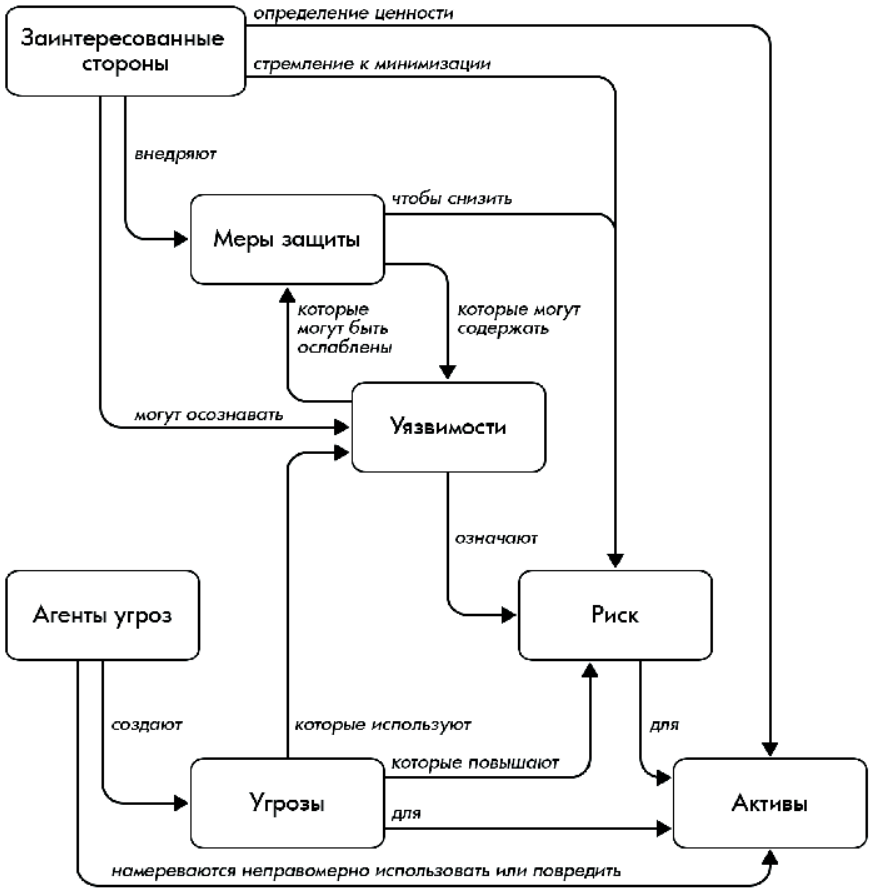
Тезаурус кибербезопасности интегрирован с понятиями информационной безопасности, безопасности приложений, сетевой безопасности, безопасности Интернет, а также безопасности критической информационной инфраструктуры.

Безопасность приложений определяется в отношении программных приложений, а также информационно-программных ресурсов и процессов, участвующих в их жизненном цикле. Безопасность сетей связана с проектированием, внедрением и использованием сетей внутри организации, между организациями, между организациями и пользователями. Безопасность в сети Интернет касается интернет-услуг и соответствующих систем информационно-коммуникационных технологий и сетей. Безопасность критической информационной инфраструктуры характеризует защищенность от соответствующих угроз, в том числе угроз информационной безопасности. Иллюстрация соотношения названных понятий (как ее увидели в международном комитете ISO JTC 1) представлена на рис.2.

По аналогии с понятием «владелец информации» в обеспечении кибербезопасности ключевую роль играют так называемые заинтересованные стороны (stakeholders), определяющие сферу

Источник: ISO 27032:2012

***Рис. 2**. Положение кибербезопасности относительно других сфер безопасности*



Источники: ISO 27032:2012, ISO 15408-1:2009

Рис. 3. *Основные понятия безопасности и характер связей между ними*

защиты своих собственных активов и другие интересы в киберпространстве. В глобальном плане киберпространство не является чьей-либо собственностью: каждый может стать его участником - заинтересованной стороной.

В качестве основных групп заинтересованных сторон выделены следующие:

1. Потребители, которые могут быть физическими лицами либо частными или общественными (государственными) организациями;

2. Провайдеры, основными из которых могут быть провайдеры интернет-доступа и провайдеры интернет-приложений.

Потребитель может стать провайдером путем создания доступных виртуальных продуктов или услуг для других пользователей киберпространства. В стандарте приведены примеры ролей заинтересованных сторон, что удобно при внедрении ролевого метода управления доступом в рамках системы обеспечения кибербезопасности.

Заметим, что стандарт регулирует вопросы безопасности с точки зрения организации, то есть он касается пользователей только в качестве клиентов или сотрудников организации, связанных с последней некоторыми соглашениями.

Как известно, к активам в области безопасности традиционно относят все, что представляет ценность, например, информационные и программные ресурсы. Несмотря на «виртуальный» акцент в определении кибербезопасности, в стандарте активы могут быть как виртуальными так и физическими, например: виртуальный аватар и физическое устройство - usb-идентификатор.

Разделяют две группы активов:

- персональные активы (например, данные личной банковской карты);

- активы организации (например, URL-адрес организации).

Соответственно таксономия киберугроз имеет традиционную схему, которая включает классификации по видам и типам активов, внешним и внутренним признакам, целям, источникам и т.д.

Онтология кибербезопасности представлена на рис.3, который представляет собой адаптацию соответствующей схемы из ISO/IEC 15408-1. Как видно из рисунка, более пристальное внимание в области кибербезопасности уделяется злонамеренным угрозам.

Руководящие указания для заинтересованных сторон

В целях планирования обеспечения кибербезопасности стандарт представляет три руководства:

- рекомендации по оценке и отработке рисков,
- рекомендации по соблюдению требований безопасности пользователями,
- рекомендации по обеспечению кибербезопасности для организаций-провайдеров.

Рекомендации по оценке и обработке рисков опираются на ISO 27005, акцентируя лишь внимание на особенностях кибербезопасности, например, необходимости принятия дополнительной ответственности в отношении заинтересованных лиц в области кибербезопасности в плане отчетности, информированности, учета разных законодательных аспектов, обеспечения согласованности действий потребителей и провайдеров на случай инцидентов и мероприятий по обеспечению безопасности.

Рекомендации для пользователей составляют совокупность норм поведения, определенных провайдером, а именно:

- понимание политики безопасности сайта или приложения,
- понимание рисков безопасности,
- соблюдение политики безопасности персональных данных,
- управление безопасностью личных данных,
- информирование уполномоченных органов о подозрительных явлениях или сообщениях,
- проверка подлинности и понимание политики безопасности торговых площадок (в случае осуществления виртуальной торговой сделки),
- контролирование целостности используемого и разрабатываемого программного обеспечения,
- обеспечение безопасности онлайн-публикаций и блогов,
- соблюдение корпоративной политики информационной безопасности в киберпространстве,
- незамедлительное информирование уполномоченных органов о личных нарушениях безопасности.

Руководящие указания организациям предлагают широкий комплекс мероприятий по управлению информационной безопасностью организацией, а именно:

- внедрение и сертификация системы менеджмента информационной безопасности,
- предоставление безопасных продуктов, прошедших соответствующую оценку,
- тестирование, мониторинг сетей и реагирование,
- техподдержка,
- поддержание уровня собственной осведомленности относительно новейших разработок,
- повышение осведомленности пользователей,
- контроль соблюдения политики безопасности и т.д.

Меры обеспечения кибербезопасности

Конкретные меры обеспечения кибербезопасности могут быть определены по результатам оценки рисков и в рамках планирования действий по повышению безопасности активов. Стандарт представляет ряд базовых мер, направленных на решение задач (табл.1):

- обеспечения безопасности приложений,
- обеспечения безопасности серверов,
- обеспечения безопасности конечных пользователей,
- защиты от атак методами социальной инженерии,
- повышения готовности.

Детального рассмотрения заслуживают мероприятия, касающиеся повышения готовности систем, представленные в отдельном приложении к стандарту:

- мониторинг darknet-сетей,
- «синкхолинг»,
- обратная трассировка.

Напомним, darknet («пустая сеть») – подмножество публичных IP-адресов, которые не используются организацией для реальной работы. Обращение к данному подмножеству адресов, таким образом, возможно лишь в результате ошибок конфигурации или нелигитимных действий, например, в целях первичной разведки путем сканирования. В стандарте описаны три варианта darknet-мониторинга:

- метод по типу «черной дыры» (black hole),
- метод слабого взаимодействия,
- метод сильного взаимодействия.

Синкхолинг (sinkhole-метод, метод «сливной трубы») представляет собой способ перенаправления подозрительного IP-трафика в альтернативное «сливное» устройство (как правило, маршрутизатор) с целью пересылки трафика DDoS-атак, блокировки и анализа бот-сетей и др. Недостатком синкхолинга является то, что атакуемый IP-адрес не может использоваться для связи с легитимными пользователями, пока маршрут не будет удален.

Методы обратной трассировки (traceback) включают методы реконструирования маршрутов атак и обнаружения местоположения узловых центров злоумышленников путем корректировки

Таблица 1

Базовые меры кибербезопасности

Категория безопасности	Мера безопасности
Безопасность приложений	Уведомление пользователей о политике безопасности
	Защита сессий веб-приложений
	Контроль корректности вводимых данных (защита от SQL-инжекций)
	Обеспечение безопасности скриптов (защита от атак межсайтового скриптинга)
	Аудит кода и независимое тестирование программного кода
	Подтверждение подлинности провайдера для потребителей
Безопасность серверов	Безопасное конфигурирование серверов
	Установка системы обновлений безопасности
	Контроль системных журналов
	Защита от вредоносных программ
	Регулярное сканирование контента на наличие вредоносных программ
	Регулярное сканирование уязвимостей сайта и приложений
	Обнаружение попыток взлома
Безопасность конечных пользователей	Использование рекомендованных версий операционных систем
	Использование рекомендованных версий программных приложений
	Использование антивирусных средств
	Настройка веб-браузеров в безопасном режиме
	Блокировка или безопасное выполнение скриптов
	Использование фильтров фишинга
	Использование дополнительных механизмов безопасности веб-браузеров
	Использование персональных межсетевых экранов и систем обнаружения вторжений
	Использование автоматических обновлений доверенных программ
Защита от атак методами социальной инженерии	Разработка и внедрение политик безопасности
	Категорирование и классификация информации
	Обучение и повышение осведомленности пользователей
	Тестирование сотрудников
	Мотивация и стимулирование сотрудников
	Использование технических механизмов контроля
Повышение готовности	Использование ловушек в «пустой» сети
	Перенаправление вредоносного трафика
	Обратная трассировка

маршрутной информации, отслеживания маркированных пакетов, аудита журналов и т.д. Наиболее проблемной является междоменная обратная трассировка по причине необходимости решения вопросов совместимости протоколов и архитектур, технических и организационных вопросов обработки информации конфиденциального характера и др.

Основы обмена информацией и координации

Создание системы обмена информацией и координации обусловлено необходимостью оперативного реагирования на инциденты кибербезопасности, которые зачастую пересекают границы организаций и государств.

В рамках информационного взаимодействия в стандарте выделяются два типа участников:

- организации, предоставляющие информацию;
- организации, получающие информацию.

Участники могут совмещать указанные целевые функции и объединяться в разные цепочки.

Организации, предоставляющие информацию, играют первичную роль и определяют классификацию информации, уровни событий безопасности, формы возможного обмена и т.д. Принимающая сторона в соответствии с принятыми соглашениями проводит мероприятия по защищенной обработке информации.

Реализация системы обмена информацией и координации требует:

***Рис. 4**. Четырехуровневая модель кибербезопасного межорганизационного взаимодействия*

- разработки политики безопасности,
- разработки и внедрения соответствующих методов и процедур,
- определения участвующих групп лиц и организаций,
- разработки и реализации соответствующих технических решений.

Стандарт предлагает варианты интерпретации известных «хороших практик» в области информационной безопасности. Например, политика безопасности должна включать принципы классификации и минимизации информации, ограничения аудитории, протокол координации и др., а процедуры должны содержать методику классификации и категорирования, подписание соглашений о неразглашении, использование заданных стандартов, тестирование и т.д. Работа с персоналом подразумевает информирование, обучение, формирование контактов и т.д.

В качестве основных технических решений отмечаются следующие: принятие стандартов форматов данных, визуализацию данных, использование криптографических механизмов, резервного копирования и других защищенных механизмов информационного обмена, также подчеркивается необходимость тестирования технических средств. Общий порядок организации защищенного информационного взаимодействия предлагается следующий:

1. Идентификация участников информационного обмена, формальная или неформальная;
2 . Определение ролей всех участников информационного обмена;
3. Выбор взаимовыгодных механизмов управления;
4. Классификация и категорирование информации;
5. Разработка политик безопасности;
6. Выбор необходимых методов и процессов для каждой из категорий информации;
7. Определение критериев эффективности, подписание соглашений о неразглашении;
8. Выбор необходимых стандартов и технических решений;
9. Подготовка к работе, установление контактов, обучение участников взаимодействия;
10. Периодическое тестирование;
11. Анализ результатов тестирования с целью оптимизации.

Гармонизация стандарта по кибербезопасности

Положения стандарта ISO 27032 опираются на организационно-технические меры, определенные, главным образом, в стандартах 27000-серии, ссылаются на подходы к оценке безопасности продукции и систем по линии «Общих критериев», а также ссылаются на рекомендации ITU (Международный союз электросвязи)[1].

В нашей стране сложилась представительная нормативная база информационной безопасности, которая может быть полезна при решении задач кибербезопасности. В таблице 2 приведены примеры национальных стандартов, гармонизированных с ISO 27032.

---

1. Рекомендации МСЭ-Т X.1500. Методы обмена информацией о кибербезопасности. МСЭ, 2012. 36 с.; Рекомендации МСЭ-Т X.1205. Обзор кибербезопасности. МСЭ, 2008. 64 с.

Таблица 2.

Национальные стандарты в области информационной безопасности

Обозначение ГОСТ	Наименование
Системы менеджмента информационной безопасности	
ГОСТ Р ИСО/МЭК 27000-2012	ИТ. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология
ГОСТ Р ИСО/МЭК 27001-2006	ИТ. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования
ГОСТ Р ИСО/МЭК 27002-2012	ИТ. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности
ГОСТ Р ИСО/МЭК 27003-2012	ИТ. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности
Управление рисками	
ГОСТ Р ИСО/МЭК 27005-2010	ИТ. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности
Оценка безопасности	
ГОСТ Р ИСО/МЭК 15408-2012	ИТ. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий
ГОСТ Р ИСО/МЭК 18045-2013	ИТ. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий
ГОСТ Р ИСО/МЭК ТО 19791-2008	ИТ. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем
Гарантии безопасности	
ГОСТ Р ИСО/МЭК 15026-2002	ИТ. Уровни целостности систем и программных средств
Сетевая безопасность	
ГОСТ Р ИСО/МЭК 27033-1-2011	ИТ. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции
Безопасность приложений	
проект ГОСТ Р (согласно планам ТК 362)	Требования по обеспечению безопасности разработки программного обеспечения
Обеспечение непрерывности бизнеса	
ГОСТ Р ИСО/МЭК 27031-2012	ИТ. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса
ГОСТ Р ИСО/МЭК ТО 18044-2007	ИТ. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности
ГОСТ Р 53647.4-2011	Менеджмент непрерывности бизнеса. Руководящие указания по обеспечению готовности к инцидентам и непрерывности деятельности
Проектирование систем безопасности	
ГОСТ Р ИСО/МЭК 21827-2010	ИТ. Методы и средства обеспечения безопасности. Проектирование систем безопасности. Модель зрелости процесса

Заключение

Международный стандарт ISO 27032-2012 дает нам ценные указания и перечень мер по повышению кибербезопасности в Интернет, придерживаясь в целом риск-ориентированного подхода в области информационной безопасности.

Использование рекомендаций стандарта, видимо, поможет организациям-поставщикам интернет-услуг спланировать работы по повышению уровня информационной безопасности ресурсов компьютерных систем, подключенных к сетям общего доступа.

Специфическими особенностями стандарта можно назвать следующие:

- относительная ограниченность области определения стандарта так называемой виртуальной киберсредой,
- решение задач повышения готовности исключительно путем противодействия злонамеренным угрозам,
- обеспечение кибербезопасности возложено на организации-провайдеры,
- обмен информацией и координация действий организаций является приоритетной задачей обеспечения кибербезопасности.

В то же время стандарт дает весьма узкое по-

нимание дефиниции кибербезопасности, существенно отличающееся от понятийного аппарата, например, в области кибервойн и кибероборонны.

Нельзя не отметить, что, на наш взгляд, первая версия стандарта во многом представляет фрагментарную интерпретацию традиционных организационно-технических мер, зачастую мало систематизированных и неполных, что является основной причиной малой распространенности стандарта.

Литература

1. Безкоровайный М.М., Лосев С.А., Татузов А.Л. Кибербезопасность в современном мире: термины и содержание // Информатизация и связь. 2011. № 6. С. 27-33.
2. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 1) // Вопросы кибербезопасности. 2013. № 1(1). С.2-9.
3. Зубарев И.В., Жидков И.В., Кадушкин И.В. Кибербезопасность автоматизированных систем управления военного назначения // Вопросы кибербезопасности. 2013. № 1(1). С.10-16.
4. Казарин О.В., Тарасов А.А. Современные концепции кибербезопасности ведущих зарубежных государств // Вестник Российского государственного гуманитарного университета. 2013. № 14. С. 58-74.
5. Корченко А.Г., Бурячок В.Л., Гнатюк С.А. Кибернетическая безопасность государства: характерные признаки и проблемные аспекты // Безпека інформації. 2013. Т. 1. № 19. С. 40-44.
6. Старовойтов А.В. Кибербезопасность как актуальная проблема современности // Информатизация и связь. 2011. № 6. С. 4-7.
7. Шеремет И.А. Информационная и кибербезопасность: интервью. Редакция «Эхо Москвы», 2013. URL: http://echo.msk.ru/programs/arsenal/1208183-echo/ (Дата обращения: 23.02.2014).
8. Штитилис Д., Клишаускас В. Особенности правового регулирования кибербезопасности в национальных законах Литвы, России и США: стратегии кибербезопасности // Вопросы российского и международного права, 2013, № 7-8, С. 80-100.
9. Юсупов Р.М., Пальчун Б.П. Безопасность компьютерной инфосферы систем критических приложений // Вооружение. Политика. Конверсия. 1993. №3. С. 23-31.
10. Walls A., Perkins E., Weiss J. Definition: Cybersecurity. Gartner. 2013. ID:G00252816. 4 p.
11. Дорофеев А.В., Шахалов И.Ю. Основы управления информационной безопасностью современной организации // Правовая информатика. 2013. №3. С.4-14.
12. Марков А.С., Цирлов В.Л. Управление рисками - нормативный вакуум информационной безопасности // Открытые системы. СУБД. 2007. № 8. С. 63-67.

References

1. Bezkorovaynyy M.M., Losev S.A., Tatuzov A.L. Kiberbezopasnost v sovremennom mire: terminy i soderzhaniye, Informatizatsiya i svyaz, 2011, No 6, pp. 27-33.
2. Borodakiy Yu.V., Dobrodeyev A.Yu., Butusov I.V. Kiberbezopasnost kak osnovnoy faktor natsionalnoy i mezhdunarodnoy bezopasnosti KhKhI veka (Chast 1), Voprosy kiberbezopasnosti, 2013, No 1(1), pp. 2-9.
3. Zubarev I.V., Zhidkov I.V., Kadushkin I.V. Kiberbezopasnost avtomatizirovannykh sistem upravleniya voyennogo naznacheniya , Voprosy kiberbezopasnosti, 2013, No 1(1), pp. 10-16.
4. Kazarin O.V., Tarasov A.A. Sovremennyye kontseptsii kiberbezopasnosti vedushchikh zarubezhnykh gosudarstv, Vestnik Rossiyskogo gosudarstvennogo gumanitarnogo universiteta, 2013, No 14, pp. 58-74.
5. Korchenko A.G., Buryachok V.L., Gnatyuk S.A. Kiberneticheskaya bezopasnost gosudarstva: kharakternyye priznaki i problemnyye aspekty, Bezpeka informatsii, 2013, Vol. 1, No 19, pp. 40-44.
6. Starovoytov A.V. Kiberbezopasnost kak aktualnaya problema sovremennosti, Informatizatsiya i svyaz. 2011. No 6, pp. 4-7.
7. Sheremet I.A. Informatsionnaya i kiberbezopasnost: intervyu. Redaktsiya "Ekho Moskvy", 2013. URL: http://echo.msk.ru/programs/arsenal/1208183-echo/
8. Stitilis D., Klisauskas V. Osobennosti pravovogo regulirovaniya kiberbezopasnosti v natsionalnykh zakonakh Litvy, Rossii i SShA: strategii kiberbezopasnosti, Voprosy rossiyskogo i mezhdunarodnogo prava (Matters of Russian and International Law), 2013, No 7-8, pp. 80-100.
9. Yusupov R.M., Palchun B.P. Bezopasnost kompyuternoy infosfery sistem kriticheskikh prilozheniy, Vooruzheniye. Politika. Konversiya, 1993, No 3, pp. 23-31.
10. Walls A., Perkins E., Weiss J. Definition: Cybersecurity. Gartner. 2013. ID:G00252816. 4 p.
11. Dorofeyev A.V., Shakhalov I.Yu. Osnovy upravleniya informatsionnoy bezopasnostyu sovremennoy organizatsii, Pravovaya informatika, 2013, No 3, pp.4-14.
12. Markov A.S., Tsirlov V.L. Upravleniye riskami - normativnyy vakuum informatsionnoy bezopasnosti, Otkrytyye sistemy. SUBD (Open Systems Journal), 2007, No 8, pp. 63-67.