АКТУАЛИЗИРОВАННЫЙ КЛАССИФИКАТОР ИНФОРМАЦИОННЫХ УГРОЗ С УЧЕТОМ МНЕНИЯ ЭКСПЕРТОВ НАУЧНО-ТЕХНИЧЕСКОЙ СФЕРЫ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.Б. Логунов, нач. отд. ФГБНУ НИИ РИНКЦЭ, канд. экон. наук, *ivley@extech.ru*
Е.А. Марышев, зам. дир. центра ФГБНУ НИИ РИНКЦЭ, канд. техн. наук, *emarysh@extech.ru*
Н.А. Миронов, дир. центра ФГБНУ НИИ РИНКЦЭ, канд. техн. наук, *namir@extech.ru*

Рассматриваются вопросы классификации информационных угроз, предложены виды информационных угроз и подход к построению классификатора угроз. Для каждого вида информационных угроз предложены классификационные признаки.

Ключевые слова: информационные угрозы, информационная безопасность, виды угроз, классификатор, классификационные признаки.

ACTUALIZED CLASSIFIER OF INFORMATION THREATS TAKING INTO ACCOUNT OPINION OF EXPERTS OF THE SCIENTIFIC AND TECHNOLOGICAL SPHERE IN THE FIELD OF INFORMATION SECURITY

A.B. Logunov, Head of Department, SRI FRCEC, Doctor of Economics, *ivley@extech.ru*
E.A. Marishev, Deputy Director of Centre, SRI FRCEC, Doctor of Engineering, *emarysh@extech.ru*
N.A. Mironov, Director of Centre, SRI FRCEC, Doctor of Engineering, *namir@extech.ru*

The article deals with the issues of classification of information threats, proposed types of information threats and approach to the construction of the classifier threats. For each type of information threats classification features are proposed.

Keywords: Information threats, information security, types of threats, classifier, classification features.

Борьба с угрозами информационной безопасности приобретает особую остроту в связи с отсутствием или недостаточностью существующего методического обеспечения оценки враждебного использования информационно-коммуникационных технологий (далее – ИКТ). Методическое обеспечение оценки враждебного использования ИКТ, в свою очередь, предполагает наличие классификатора угроз в области информационной безопасности, включающего классифицирующие признаки их враждебного использования.

В принятом в 2013 г. в России документе «Основы государственной политики в области международной информационной безопасности до 2020 года» под международной информационной безопасностью понимается такое состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной информационной инфраструктуры [1]. Таким образом, понятие информационной безопасности включает политико-идеологические аспекты (манипулирование информацией, пропаганда посредством глобальных информационных сетей, информационное воздействие) и технические аспекты (безопасность информационных сетей и систем). Другими словами, информационная безопасность охватывает интересы

личности, общества и государства в информационном пространстве, включающем как информационно-телекоммуникационную инфраструктуру, так и саму информацию.

При этом следует отметить, что западные страны, прежде всего США, придерживаются узкого подхода, ограничивая проблемы и угрозы, исходящие из информационного пространства, лишь областью киберугроз. Такой подход к классификации информационных угроз ярко проявляется и в классификаторах, разработанных за рубежом.

Один из первых классификаторов компьютерных преступлений создан в 1991 г. и в настоящее время используется национальными бюро Интерпола более чем ста стран. Этот классификатор положен в основу автоматизированной информационно-поисковой системы и предусматривает 26 групп компьютерных преступлений, сведенных в шесть видов: 1) QA – несанкционированный доступ и перехват; 2) QD – изменение компьютерных данных; 3) QF – компьютерное мошенничество; 4) QR – незаконное копирование; 5) QS – компьютерный саботаж; 6) QZ – прочие компьютерные преступления.

В 2009 г. консорциумом европейских университетов The FORWARD была разработана классификация под названием «Белая книга: новые угрозы для ИКТ» [2]. Эксперты определили 28 угроз, которые были распределены по восьми категориям. В качестве направлений развития угроз в киберпространстве были выделены: новые технологии, новые приложения, новые бизнес-модели и новая социальная динамика.

По мнению экспертов, наибольший приоритет имеют следующие пять угроз:

– угрозы, связанные с параллелизмом вычислений, выполняемых новыми процессорами;

– угрозы, обусловленные наличием огромного числа устройств, подключенных к сети, объемом и сложностью пакетов программного обеспечения;

– угрозы со стороны структур поддержки теневой экономики;

– угрозы от вредоносных программ для мобильных устройств;

– угрозы, связанные с социальными сетями.

При этом, полагают они, современный этап характеризуется возрастанием угроз, связанных с психологическим или физиологическим воздействием на органы человека носимой электроникой, «интернетом вещей», облачными технологиями, интеллектуальными транспортными системами и средствами управления «умными домами».

По мнению основателя компании «Лаборатория Касперского» Е. Касперского, в настоящее время к самым серьезным киберугрозам относятся [3]:

– кибервойны и кибероружие, несущие деструктивный потенциал для информационной инфраструктуры;

– использование социальных сетей для манипулирования массами;

– интернет-зависимость молодого поколения;

– разработка вредоносного ПО, масштабы которой растут год от года;

– проблема исчезновения приватности и уничтожение понятия неприкосновенности частной жизни.

В действующей редакции Доктрины информационной безопасности Российской Федерации, утвержденной Президентом РФ в 2000 г., определены четыре вида угроз информационной безопасности РФ [4]:

– угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;

– угрозы информационному обеспечению государственной политики РФ;

– угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;

– угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

С учетом современных тенденций и мнения отечественных экспертов научно-технической сферы в области информационной безопасности нами предлагается проект расширенного классификатора угроз, включающего три основных группы угроз:

– угрозы информационной безопасности государства;

– угрозы информационной безопасности общества и личности;

– угрозы безопасности технических средств информационно-телекоммуникационных систем (далее – ИТКС).

Каждая из трех групп, в свою очередь, подразделяется на виды угроз. В частности, группа угроз информационной безопасности государства может содержать семь видов угроз:

– информационные угрозы проведению государственной политики;

– информационные угрозы целостности государства;

– информационные угрозы международной деятельности государства;

– информационные угрозы научно-техническим ресурсам государства;

– угрозы развитию национальной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи;

– угрозы обеспечению потребностей внутреннего рынка в национальной продукции;

– угрозы обеспечению накопления, сохранности и эффективного использования национальных информационных ресурсов.

Группа угроз враждебного использования ИКТ, направленных против информационной безопасности общества и личности, включает три вида:

– угрозы информационному обеспечению деятельности общественных объединений, коллективов и отдельных их представителей;

– информационные угрозы правам и свободам человека в области духовной жизни;

– информационные угрозы индивидуальному, групповому и общественному сознанию.

Группа угроз враждебного использования ИКТ, направленных против технических средств ИТКС, может включать также три вида угроз:

– угрозы информационной безопасности существующих информационных и телекоммуникационных систем общего назначения;

– угрозы информационной безопасности информационных и телекоммуникационных систем специального назначения;

– угрозы информационной безопасности создаваемых информационно-телекоммуникационных систем.

Структура классификатора угроз информационной безопасности приведена на рисунке.

Каждый из рассмотренных выше видов угроз информационной безопасности характеризуется классификационными признаками. Рассмотрим подробнее классификационные признаки, раскрывающие содержание видов угроз и подлежащих наблюдению и фиксации в системах контроля информационной безопасности.

Информационные угрозы проведению государственной политики характеризуются следующими признаками:

– монополизация информационного рынка, его отдельных секторов национальными и зарубежными информационными структурами;

– деформация системы массового информирования за счет монополизации средств массовой информации и неконтролируемого расширения сектора зарубежных средств массовой информации в национальном информационном пространстве;

– блокирование деятельности государственных средств массовой информации по информированию национальной и зарубежной аудитории;

– снижение эффективности информационного обеспечения государственной политики вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики;

– распространение дезинформации о политике государства, деятельности федеральных органов государственной власти, событиях, происходящих в стране и за рубежом;

– блокирование деятельности национальных средств массовой информации по разъяснению зарубежной аудитории целей и основных направлений национальной государственной политики;

– информационное воздействие иностранных политических, экономических, военных и информационных структур на разработку и реализацию стратегии внешней и внутренней политики государства;

– распространение за рубежом дезинформации о внешней и внутренней политике государства.

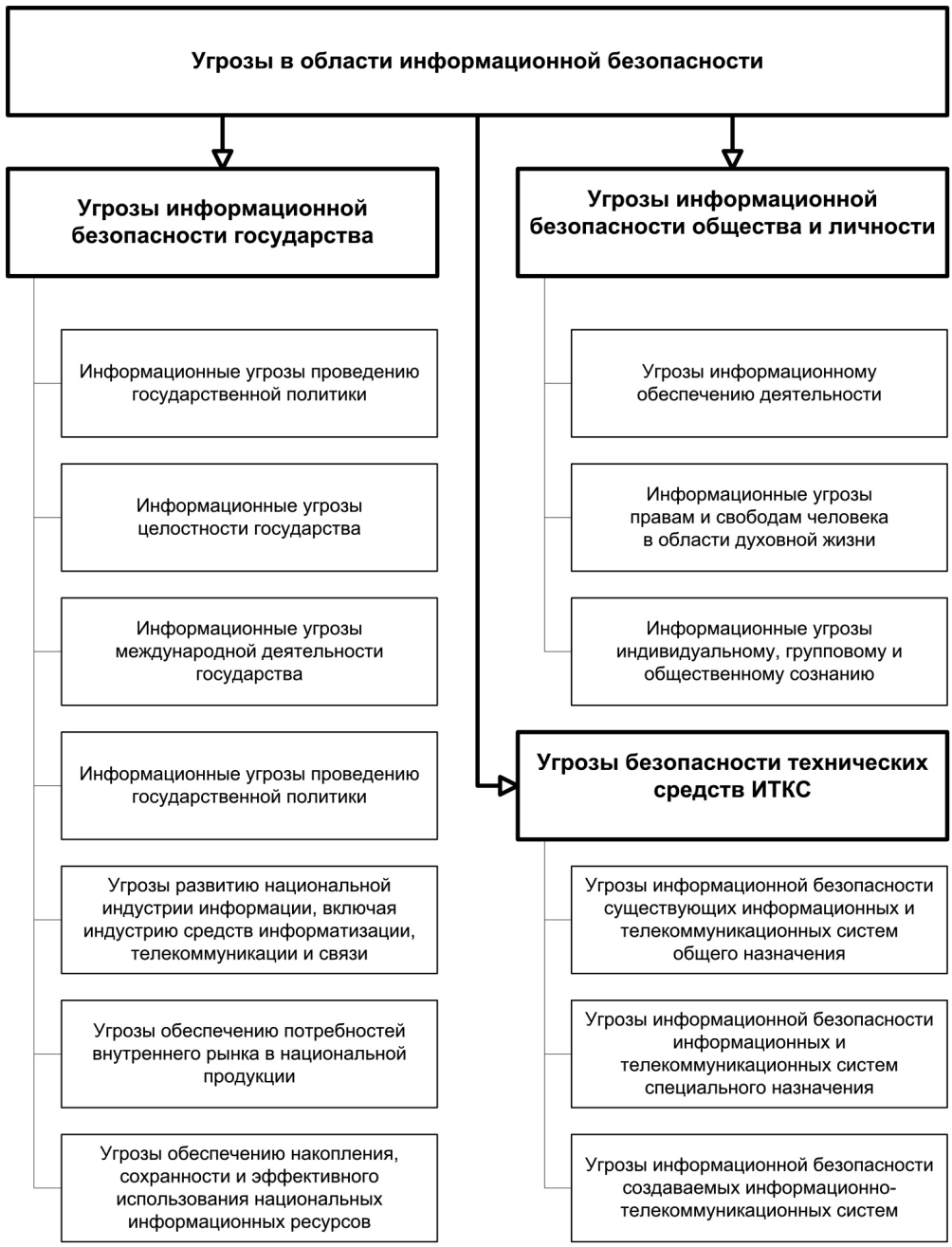

Рис. 1. Виды угроз информационной безопасности

Информационные угрозы целостности государства включают следующие признаки:

– использование средств массовой информации для пропаганды антигосударственных идей экстремистских организаций;

– деятельность общественных объединений, направленная на насильственное изменение государственного строя и нарушение целостности государства;

– разжигание социальной, расовой, национальной и религиозной вражды, распространение этих идей в средствах массовой информации;

– блокирование деятельности национальных средств массовой информации по доведению до зарубежной аудитории национального мнения по социально значимым событиям национальной и международной жизни;

– использование зарубежными специальными службами средств массовой информации, действующих на территории государства, для нанесения ущерба национальной обороноспособности страны и безопасности;

– деятельность иностранных политических, экономических и военных структур, направленная против интересов государства в сфере обороны;

– информационно-пропагандистская деятельность, подрывающая престиж национальных силовых структур и их боеготовность;

– распространение дезинформации;

– разведывательная деятельность зарубежных государств;

– диверсионно-подрывная деятельность специальных служб иностранных государств, осуществляемая методами информационно-психологического воздействия.

Классификационными признаками информационных угроз международной деятельности государства являются:

– нарушение прав граждан и юридических лиц в информационной сфере за рубежом;

– попытки несанкционированного доступа к информации и воздействия на информационные ресурсы, информационную инфраструктуру национальных органов исполнительной власти, реализующих внешнюю политику государства, национальных представительств и организаций за рубежом, национальных представительств в международных организациях;

– нарушение установленного порядка сбора, обработки, хранения и передачи информации в национальных органах власти, реализующих внешнюю политику, и на подведомственных им предприятиях, в учреждениях и организациях;

– информационно-пропагандистская деятельность политических сил, общественных объединений, средств массовой информации и отдельных лиц, искажающая стратегию и тактику национальной внешнеполитической деятельности;

– недостаточная информированность населения о национальной внешнеполитической деятельности.

Классификационными признаками информационных угроз научно-техническим ресурсам государства являются:

– попытки противоправного доступа иностранных государств к национальным научно-техническим ресурсам в области ИКТ для использования в собственных интересах;

– действия по разрушению научно-технического пространства объединений государств за счет переориентации на западные страны их научно-технических связей и наиболее перспективных научных коллективов;

– активизация деятельности иностранных государственных и коммерческих предприятий, учреждений и организаций в области промышленного шпионажа с привлечением к ней разведывательных и специальных служб;

– информационно-технические воздействия на объекты научно-технической инфраструктуры (в том числе радиоэлектронная борьба, проникновение в компьютерные сети).

Угрозы развитию национальной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, характеризуются следующими признаками:

– противодействие доступу национальных структур к новейшим информационным технологиям;

– противодействие взаимовыгодному и равноправному участию национальных производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов;

– создание условий для усиления национальной технологической зависимости в области современных информационных технологий;

– стремление развитых стран ограничить развитие национального научно-технического потенциала в области ИКТ (скупка акций передовых предприятий с их последующим перепрофилированием, сохранение экспортно-импортных ограничений и тому подобное).

Угрозы обеспечению потребностей внутреннего рынка в национальной продукции проявляются в следующих признаках:

– закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии национальных аналогов, не уступающих по своим характеристикам зарубежным образцам;

– вытеснение с внутреннего рынка национальных производителей средств информатизации, телекоммуникации и связи;

– создание льготных условий на национальном рынке для иностранной научно-технической продукции.

Угрозы обеспечению накопления, сохранности и эффективного использования национальных информационных ресурсов содержатся в следующих признаках:

– увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности;

– бесконтрольная деятельность коммерческих структур по созданию и защите систем сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной и другой информации;

– нерешенность вопросов защиты интеллектуальной собственности предприятий, приводящая к утечке за рубеж ценнейших национальных информационных ресурсов;

– утечка за рубеж идей и передовых разработок в области ИКТ;

– отсутствие патентной защиты результатов научно-технической деятельности национальных ученых в области ИКТ;

– отсутствие мероприятий по защите информации, особенно на акционированных предприятиях, в научно-технических учреждениях и организациях.

Угрозы информационному обеспечению деятельности предлагается оценивать следующей совокупностью признаков:

– нарушение прав и свобод граждан, реализуемых в информационной сфере;

– принятие нормативных правовых актов, ущемляющих права и свободы граждан в области информационной деятельности;

– создание монополий на формирование, получение и распространение информации с использованием телекоммуникационных систем;

– нерациональное, чрезмерное ограничение доступа к общественно необходимой информации;

– неисполнение органами государственной власти, органами местного самоуправления, организациями и гражданами требований законодательства, регулирующего отношения в информационной сфере.

Признаками информационных угроз правам и свободам человека в области духовной жизни являются:

– принятие нормативных правовых актов, ущемляющих права и свободы граждан в области информационного обеспечения духовной жизни;

– дезорганизация и разрушение информационной системы накопления и сохранения культурных ценностей, включая архивы;

– усиление зависимости духовной, экономической и политической сфер общественной жизни от зарубежных информационных структур;

– пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих принятым в государстве ценностям;

– снижение духовного, нравственного и творческого потенциала населения, существенно осложняющее подготовку ресурсов для внедрения и использования новейших информационных и телекоммуникационных технологий;

– нарушение общественной стабильности, нанесение вреда духовному здоровью граждан вследствие деятельности религиозных объединений, проповедующих религиозный фундаментализм, а также тоталитарных религиозных сект;

– усиление негативного влияния иностранных религиозных организаций и миссионеров;

– использование эфирного времени в электронных средствах массовой информации для проката программ, пропагандирующих насилие и жестокость, антиобщественное поведение.

Информационные угрозы индивидуальному, групповому и общественному сознанию характеризуются следующими признаками:

– противоправное информационно-психологическое воздействие на массовое сознание общества;

– применение специальных средств воздействия на индивидуальное, групповое и общественное сознание;

– неправомерное ограничение доступа граждан к открытым информационным ресурсам органов государственной власти, органов местного самоуправления, к открытым архивным материалам, к другой открытой социально значимой информации;

– противодействие, в том числе со стороны криминальных структур, реализации гражданами своих прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;

– нарушение прав и свобод человека и гражданина в области массовой информации;

– вытеснение национальных информационных агентств, средств массовой информации с внутреннего информационного рынка;

– манипулирование информацией (дезинформация, сокрытие или искажение информации);

– информационные атаки рекламой, маркетингом или пропагандой.

Угрозы информационной безопасности существующих информационных и телекоммуникационных систем общего назначения предлагается характеризовать следующими признаками:

– противоправные сбор и использование информации;

– нарушения технологии обработки информации;

– разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;

– деятельность специальных служб иностранных государств, преступных сообществ, организаций, групп и отдельных лиц, направленная на осуществление контроля за функционированием информационных и телекоммуникационных систем;

– уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;

– несанкционированный доступ к информации, находящейся в банках и базах данных;

– нарушение законных ограничений на распространение информации;

– наличие технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем;

– перехват информации по техническим каналам;

– проникновение криминальных элементов в компьютерные системы и сети банков и иных кредитных организаций;

– противоправное копирование информации и ее искажение вследствие преднамеренных или случайных действий персонала;

– утечки информации по техническим каналам, возникающей при эксплуатации технических средств ее обработки, хранения и передачи;

– специальные программно-технические воздействия, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации.

Признаками угроз информационной безопасности информационных и телекоммуникационных систем специального назначения следует считать:

– уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;

– воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;

– компрометация ключей и средств криптографической защиты информации;

– утечка информации по техническим каналам;

– перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;

– деятельность специальных служб иностранных государств, преступных сообществ, организаций, групп и отдельных лиц, направленная на получение несанкционированного доступа к информации;

– нарушение технологии работы с информацией, несанкционированный доступ к ней;

– перехват информации из помещений и с объектов, а также информации, передаваемой по каналам связи с помощью технических средств;

– несанкционированный доступ к обрабатываемой или хранящейся в технических средствах информации;

– нарушение конфиденциальности информации при взаимодействии информационных и телекоммуникационных систем различных классов защищенности;

– нарушение установленного регламента сбора, обработки, хранения и передачи информации, находящейся в оборонных формированиях, ведомствах и учреждениях, на предприятиях оборонного комплекса;

– преднамеренные действия, а также ошибки персонала информационных и телекоммуникационных систем специального назначения;

– ненадежное функционирование информационных и телекоммуникационных систем специального назначения.

Угрозы информационной безопасности создаваемых информационно-телекоммуникационных систем характеризуются следующими признаками:

– внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;

– привлечение к работам по созданию, развитию и защите информационных и телекоммуникационных систем организаций и фирм, не имеющих государственных лицензий на осуществление этих видов деятельности;

– использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии информационной инфраструктуры;

– внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;

– разглашение информации, содержащей техническую и коммерческую тайну;

– внедрение на объекты и в технические средства электронных устройств перехвата информации.

В заключение следует отметить, что предложенный классификатор угроз в области информационной безопасности содержит 90 классификационных признаков и существенно расширяет и актуализирует содержательную часть существующих классификаторов. Отличительной особенностью предложенного классификатора является его направленность на использование в системах анализа фактов враждебного использования информационно-коммуникационных технологий и их последующей квалификации. Информация о рассмотренных классификационных признаках информационных угроз может собираться от объектов информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, систематизироваться и анализироваться в автоматизированном режиме.

Статья подготовлена по материалам научно-исследовательской работы, выполненной ФГБНУ НИИ РИНКЦЭ по заданию № 2015/Н7 Министерства образования и науки РФ на выполнение работ в рамках государственного задания в сфере научной деятельности.

Список литературы

1. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 г. // Официальный сайт Совета безопасности РФ. Available at: http://www.scrf.gov.ru/documents/6/114.html (дата обращения 28.09.2015 г.).

2. The Forward Emerging ICT Threats Whitebook. 2010. Available at: http://www.ict-forward.eu/media/publications/forward-whitebook.pdf (дата обращения 18.09.2015 г.).

3. Евгений Касперский назвал 5 крупнейших киберугроз в мире. Available at: http://www.cnews.ru/news/top/evgenij_kasperskij_nazval_5_krupnejshih.

4. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. № Пр-1895) // Официальный сайт Совета безопасности РФ. Available at: http://www.scrf.gov.ru/documents/6/5.html.

References

1. *Osnovy gosudarstvennoy politiki Rossiyskoy Federatsii v oblasti mezhdunarodnoy infor-matsionnoy bezopasnosti na period do 2020 g. Ofitsial'nyy sayt Soveta bezopasnosti RF* [Principles of State Policy of the Russian Federation in the field of international security of information for the period up to 2020. Official site of the Security Council]. Available at: http://www.scrf.gov.ru/documents/6/114.html (the date of claim of 09.28. 2015).

2. The Forward Emerging ICT Threats Whitebook. 2010. Available at: http://www.ict-forward.eu/media/publications/forward-whitebook.pdf (the date of claim of 09.18.2015).

3. *Evgeniy Kasperskiy nazval 5 krupneyshikh kiberugroz v mire* [Evgeny Kaspersky named the top 5 of the world of cyber threats]. Available at: http://www.cnews.ru/news/top/evgenij_kasperskij_nazval_5_krupnejshih.

4. *Doktrina informatsionnoy bezopasnosti Rossiyskoy Federatsii (utv. Prezidentom RF ot 9 sentyabrya 2000 g. № Pr-1895). Ofitsial'nyy sayt Soveta bezopasnosti RF* [Information Security Doctrine of the Russian Federation (approved by. The President of the Russian Federation dated September 9, 2000 № Pr-1895). Official site of the Security Council]. Available at: http://www.scrf.gov.ru/documents/6/5.html.