КИБЕРУЧЕНИЯ: МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ENISA

***Петренко Александр Анатольевич**, кандидат технических наук, доцент, г. Москва*
***Петренко Сергей Анатольевич**, доктор технических наук, профессор, Санкт-Петербург*

28 апреля 2014 года Евросоюз (ЕС) провел очередные киберучения Cyber Europe 2014 (CE 2014), которые, по мнению организатора – Европейского агентства сетевой и информационной безопасности (ENISA) – стали самыми крупномасштабными и сложными за всю историю проведения подобных мероприятий. В упомянутых киберучениях приняли участие более 600 участников – 200 представителей организаций Евросоюза и 400 экспертов – из 29 стран ЕС и ЕАСТ (Европейская ассоциация свободной торговли). Ранее 16 апреля 2014 года Европейский парламент утвердил новый мандат ENISA, подтвердив полномочия агентства до 2020 года как ведущей организации в области кибербезопасности в Евросоюзе. В статье проведен анализ передового опыты организации и проведения киберучений.

***Ключевые слова**: обучение по информационной безопасности, киберучения, кибербезопасность, компьютерные атаки, тренировки специалистов.*

CYBER EDUCATION: METHODICAL RECOMMENDATIONS ENISA

***Aleksandr Petrenko**, Ph.D., Associate Professor, Moscow*
***Sergei Petrenko**, Doctor of Science (Tech), Professor, St. Petersburg*

April 28, 2014, the European Union (EU) held a regular Cyber Europe 2014 kiberucenia (CE–2014), which, in the opinion of the organiser, the European network and information security agency (ENISA) is the most extensive and complex in the history of such events. The kiberuceniah was attended by more than 600 participants–200 representatives of European Union and 400 experts from 29 countries of the EU and EFTA (European Free Trade Association). April 16, 2014 previously, the European Parliament has approved a new mandate of ENISA, confirming the authority of the Agency until the year 2020 as the leading organi–zation in the field of cyber security in the European Union. In the article the analysis of advanced experiences of organization and conduct of the kiberucenij.

***Keywords**: information security training, kiberucenia, cyber security, computer attacks, workout spe–cialists*

Состояние вопроса

В настоящее время вопросами организации и проведения крупномасштабных национальных и международных или транснациональных киберучений занимаются ведущие международные организации:

1) Азиатско-Тихоокеанское экономическое сотрудничество (АТЭС, англ. Asia-Pacific Economic Co-operation, APEC), www.apec.org;

2) Ассоциация государств Юго-Восточной Азии (АСЕАН, Association of SouthEast Asian Nations, ASAN), www.asean.org;

3) Европейский союз (Евросоюз, ЕС, European Union, EU), www.europa.eu.

4) Совет Европы (Council of Europe), www.coe.int;

5) Европол (Europol), www.europol.europa.eu;

6) Форумпо реагированию на инциденты безопасности (Forum of Incident Response and Security Teams, FIRST), www.first.org;

7) Группа восьми (в настоящее время – семи) (Group of eight, G8, www.g8russia.ru;

8) Институт инженеров по электротехнике и электронике (Institute of Electrical and Electronics Engineers, IEEE), www.ieee.org;

9) Международная электротехническая комиссия (МЭК, International Electrotechnical Commission, IEC), www.iec.ch;

10) Международная организация по стандарти-

зации (ИСО, International Organization for Standardization, ISO), www.iso.org;

11) Международный союз электросвязи (МСЭ, International Telecommunication Union, ITU), www.itu.int;

12) Международная некоммерческая организация – Internet Corporation for Assigned Names and Numbers, или ICANN, www.icann.org;

13) Инженерный совет Интернета (Internet Engineering Task Force, IETF),www.ietf.org/about/mission.html;

14) Форум по управлению Интернетом (Internet Governance Forum, IGF), www.intgovforum.org/cms;

15) Интерпол, Interpol— сокращённое название (с 1956 года) Международной организации уголовной полиции (International Criminal Police Organization, ICPO), www.interpol.int;

16) АльянсНАТО (North Atlantic Treaty Organization, NATO); www.nato.int/cps/ru/natolive/topics_51105.html;

17) Организация американских государств (ОАГ, Organization of American states, OAS), www.oas.org.;

18) Организация экономического сотрудничества и развития (ОЭСР, Organisation for Economic Cooperation and Development, OECD),www.oecdru.org/oecd_rf.html;

19) Организации Объединенных Наций, ООН, www.un.org/ru и др.

Среди перечисленных организаций важное место занимает Европейский союз [2–4], который организует и проводит киберучения на основе ранее принятых специальных Сообщений Европейской Комиссии: *«Стратегия обеспечения безопасности ЕС в действиях: пять шагов к укреплению безопасности Европы» 2010 года, «Защита Европы от крупномасштабных кибератак и сбоев: повышение готовности, безопасности и устойчивости» 2009 года, «Стратегия безопасности информационного общества «Диалог, партнерство и расширение возможностей» 2006 года, «Сетевая и информационная безопасность: предложения для европейского подхода»* 2001 года и пр. Например, в Сообщении Европейской Комиссии 2009 года по защите критически важной инфраструктуры Евросоюза COM (2009) - 1493 было указано на актуальность и «необходимость проведения крупномасштабных киберучений». Принятая в декабре 2009 года резолюция Совета ЕС закрепила за странами ЕС право «проводить национальные киберучения», а также призвала к активному участию в международных «транснациональных киберучениях». В результате первое киберучение Евросоюза Cyber Europe 2010 было проведено 4 ноября 2010 года, а первое совместное киберучение ЕС и США Cyber Atlantic 2011 – в 2011 году [1].

К основным направлениям развития кибербезопасности, которые были определены в *Цифровой повестке дня для Европы «Доверие и безопасность» (Pillar III: Trust and Security) как составной части Стратегии «Европа 2020»)*, относятся:

1) усиление политики в сфере сетевой и информационной безопасности;

2) противодействие современным кибератакам на критические важные государственные и коммерческие информационные системы;

3) учреждение Европейской платформы по борьбе с киберпреступностью (European cybercrime platform);

4) изучение необходимости создания Европейского центра по борьбе с киберпреступностью (European cybercrime centre);

5) усиление борьбы с киберпреступностью на международном уровне;

6) поддержка готовности к действиям по обеспечению кибербезопасности на общеевропейском уровне;

7) изучение способов уведомления пользователей в случаях нарушения системы безопасности (утраты, хищения или изменения персональных данных и другой конфиденциальной информации);

8) контроль исполнения правил частной жизни в Интернете;

9) поддержка механизма уведомлений о противоправном он-лайн контенте и повышение осведомленности о безопасном Интернете для детей;

10) стимулирование корпоративного саморегулирования в области безопасных он-лайн услуг;

11) учреждение государствами-членами ЕС команд оперативного реагирования на компьютерные инциденты безопасности (pan-European CERT);

12) разработка актуальных моделей и методов противодействия современным кибератакам;

13) обеспечение государствами-членами Евросоюза работы горячих линий для получения сообщений об обнаружении вредоносного контента;

14) создание национальных систем оповещения об опасности (national alert platforms) в масштабах Евросоюза.

15) организация и проведение киберучений государствами-членами Евросоюза, а также другими странами-партнерами ЕС.

Отличительными чертами европейского подхода [8–19] является работа на принципах «множественного участия» и «открытого диалога» между различными государственными и коммерческими организациями как внутри, так и за пределами Евросоюза. Этому способствуют и принятые в ЕС принципы субсидиарности и многоуровнего управления. Данные положения нашли отражение и в соответствующей структуре регуляторов: полномочия по вопросам кибербезопасности распределены между институтами ЕС (ЕК, Парламентом,

Советом ЕС), агентствами ЕС и национальными органами. При этом проблематика кибербезопасности в ЕС перестает быть лишь вопросом внутренней безопасности: возрастающее значение приобретает внешнее измерение в рамках ОВПБ и ОПБО. Основным «союзником» ЕС в данной сфере являются США. Продолжается активное сотрудничество с НАТО и Советом Европы. Кроме того Евросоюз и государства-члены участвуют и в работе других глобальных форумов, в частности, ООН и МСЭ.

Роль ENISA

Ведущей организацией Евросоюза, ответственной за проведение киберучений, является Европейское агентство сетевой и информационной безопасности (European Network and Information Security Agency – ENISA, www.enisa.europa.eu), которое было учреждено в ноябре 2004 году и 1 сентября 2005 года приступило к работе в соответствии с регламентом ЕС № 460/2004.

Штаб-квартира ENISA находится в греческом городе Ираклион – административном центре острова Крит. В состав ENISA входит: аппарат управления, постоянные группы представителей, а также временные рабочие группы по специальным вопросам. Кроме того, государства-участники ЕС представлены в агентстве одним офицером связи от каждой из стран ЕС и Европейской экономической зоны, которые вместе с представителями от Европейской Комиссии и Совета ЕС образуют сеть национальных офицеров связи (National Liaison Officers Network). Обязанности исполнительного директора ENISA с 2009 года исполняет доктор Удо Хельмбрехт, ранее возглавлявший немецкое Федеральное управление по информационной безопасности (нем. Bundesamtfur Sicherheit in der Informationstechnik – BSI), www.bsi.bund.de/DE/Home/home_node.html.

К основным целям ENISA относятся (ст. 2 Регламента) [10]:

1) расширение возможностей Евросоюза имеждународного делового сообщества по своевременному и качественному решению проблем кибербезопасности;

2) повышение общего уровня компентенции Комиссии и стран ЕС по вопросам кибербезопасности;

3) повышение общей культуры осведомленности Евросоюза по вопросам кибербезопасности;

4) содействие Комиссии по вопросам развития законодательства в области кибербезопасности и разработки соответствующей организационно-распорядительной и технической документации.

Для достижения обозначенных целей ENISA решает следующие задачи [11–13]:

1) разрабатывает перспективные методики управления рисками кибербезопасности;

2) консультирует институты ЕС и/или уполномоченные национальные органы по вопросам кибербезопасностии;

3) осуществляет внутренние и международные программы взаимодействия с различными государственными и коммерческими партнерами по вопросам кибербезопасности;

4) разрабатывает актуальное методологическое обеспечение по вопросам кибербезопасности;

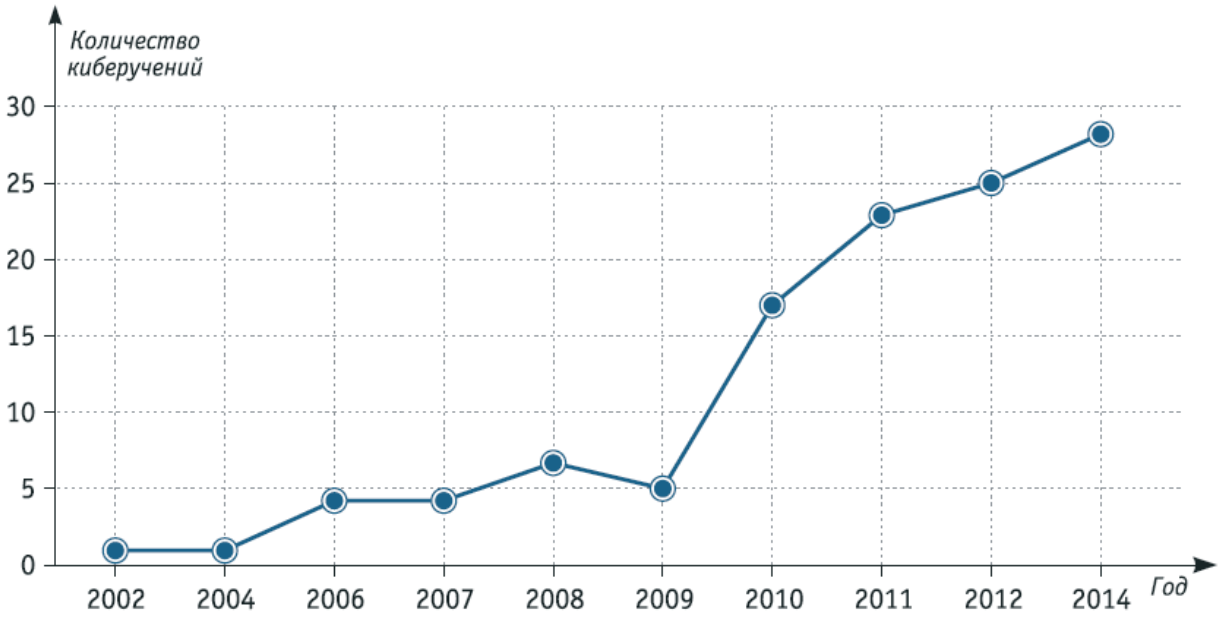

***Рис. 1**. Динамика роста количества киберучений*

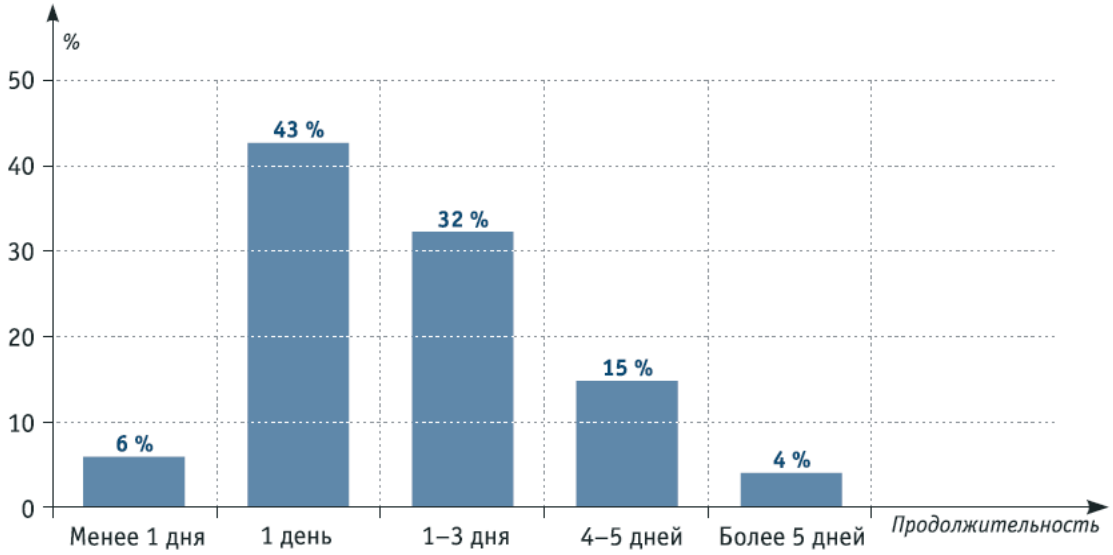

***Рис. 2**. Продолжительность киберучений*

5) реализует разнообразные программы повышения осведомленности по вопросам кибербезопасности;

6) осуществляет разработку и сопровождение стандартов кибербезопасности.

7) организует и проводит крупномасштабные транснациональные киберучения с участием стран Евросоюза, США, Японии и других стран.

Следует отметить, что при проведении киберучений существенную помощь ENISA оказывают и другие автономные агентства Евросоюза (общее количество которых – более 35), созданных в период 1994–2010 годов для решения специальных *технических, научно-исследовательских и административных задач:*

- *агентства сообщества:* служба по гармонизации внутреннего рынка – OHIM, штаб-квартира в Аликанте, Испания; агентство безопасности морского сообщения – EMSA, штаб-квартира в Лиссабоне, Португалия; агентство авиационной безопасности – EASA, штаб-квартира в Кельне, Германия и др.;

- *агентства в сфере общей внешней политики и политики безопасности:* оборонное агентство – EDA, штаб-квартира в Брюсселе, Бельгия; институт по исследованиям безопасности – EUISS, штаб-квартира в Париже, Франция; спутниковый центр – EUSC, штаб-квартира в Мадриде, Испания;

- *агентства в сфере полицейского и судебного сотрудничества по уголовным делам:* пункт судебного сотрудничества – Eurojust; полицейское ведомство Europol, обе со штаб-квартирой в Гааге, Нидерланды; полицейский колледж CEPOL, штаб-квартира в Брамсхилле, Великобритания;

- временные *исполнительные агентства:* агентство по образованию, аудиовизуальным средствам и культуре – EACEA; агентство по конкуренции и инновациям – EACI; исполнительное агентство Европейского исследовательского совета – ERC; исследовательское исполнительное агентство – REA, все со штаб-квартирой в Брюсселе, Бельгия и др.

Также, необходимо отметить помощь недавно созданного (1 января 2013 года) Центра по борьбе с киберпреступнос тью– ECCC (European Cyber Crime Centre).

К основным практическим результатам ENISA [14–19] следует отнести ряд разработанных им документов:

- «Лучшие практики» по координации и управлению европейскими центрами оперативного реагирования на инциденты кибербезопасности CERT/CSIRT (Computer Security and Incident Response Team, в том числе подготовка и поддержание в актуальном состоянии соответствующей методологической базы: «По-шагового руководства по созданию CSIRT. Примеры и контрольные таблицы в форме проектного плана. WP2006/5.1 (***CERT***-D1/D2)», а также универсального «Сборника упражнений для служб реагирования на компьютерные инциденты (CERT)», состоящего из руководства для тренеров, учебника для обучающихся и дополнительного материала для практики, содержащего 29 различных сценариев обучения, а также проведения тренингов на рабочих местах.

- «Проект национальной Стратегии кибербезопасности» в рамках Евросоюза. ENISA разработало соответствующее практическое руководство (Good Practices Guide), в котором приведены лучшие практики и рекомендации по разработке, реализации и сопровождению государственной Стратегии кибербезопасности, в том числе вопросы раз-

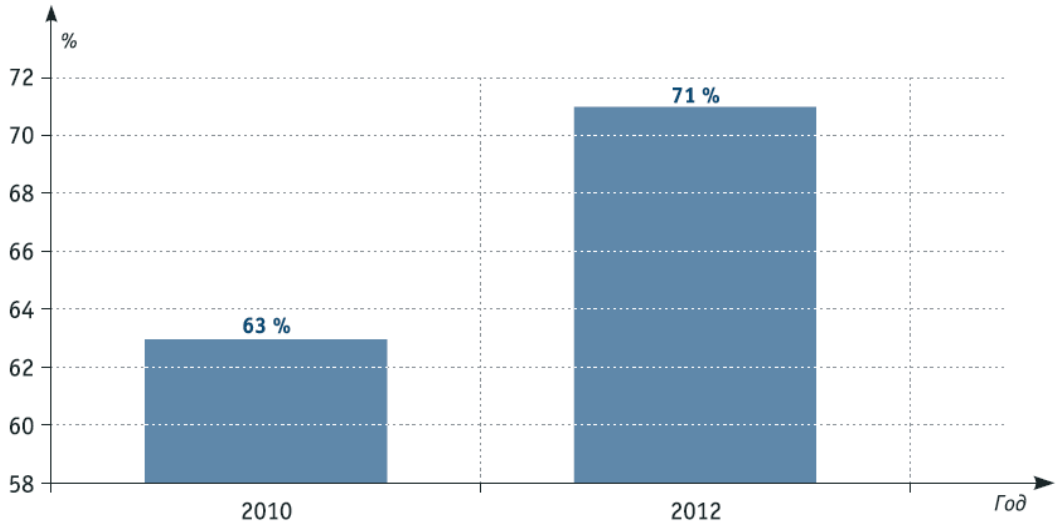

***Рис. 3**. Степень участия стран ЕС и ЕАСТ в национальных киберучениях*

работки государственной модели кибербезопасности, возможные формы общественно-государственного партнерства, разработки соответствующих политик, стандартов и регламентов, выбора соответствующих организационных и технических мер кибербезопасности и пр.

- Рекомендации по облачной безопасности. ENISA подготовила отчет под названием «Информирование об инцидентах облачной безопасности – Концепция информирования о серьезных инцидентах» (Cloud Security Incident Reporting – Framework for reporting about major cloud security incidents). Цель отчета заключается в том, чтобы дать государственным органам (министерствам, контролирующим органам, уполномоченным органам по компьютерной безопасности) представление о вопросах и проблемах, возможных схемах информирования о существенных инцидентах безопасности облачных вычислений. Для решения этих проблем и развития общеевропейской практики информирования об инцидентах для облачных провайдеров ENISA предлагает ряд рекомендаций, в том числе уполномоченным государственным и коммерческим организациям рекомендуется включать обязательства по информированию об инцидентах в требования по закупкам. Потребителям облачных услуг следует включать требования к информированию об инцидентах в соглашения о качестве услуг (SLA). Необходимо гармонизировать требования в части информирования об инцидентах на законодательном уровне и пр.

- Рекомендации по безопасности АСУ технологическими процессами (АСУ ТП): 9 октября 2013 года был опубликован официальный доклад (white paper) с рекомендациями по предотвращению кибератак на АСУ ТП и своевременному реагированию на таковые, в котором обращено внимание на необходимость реализации нового, так называемого *«проактивного процесса изучения и анализа уже произошедших инцидентов безопасности»*.

- «Лучшие практики» организации и проведения крупномасштабных транснациональных киберучений. Начиная с 2010 года ENISA проводит киберучения каждые два года. Здесь основными целями киберучений являются совершенствование законодательных и организационно-технических механизмов противодействия массовым и групповым кибератакам, а также отработка навыков коллективного противостояния упомянутым кибератакам в масштабе Евросоюза.

Фактография ENISA

Сравнительно недавно агентством ENISA был проведен критический анализ 85 киберучений, которые были организованы и проведены в период с 2002 по 2012 годы с участием более 20 стран ЕС и 60 стран-партнеров. Выявленные статистические данные и комментарии к ним представлены на рис. 1–8.

К типовым целям и задачам проведенных киберучений относились:

- повышение осведомленности по вопросам кибербезопасности;
- оценивание способности государственных и коммерческих структур к своевременному реагированию, нейтрализации и пресечению как известных, так и неизвестных кибератак;
- определение роли и места соответствующих должностных лиц, налаживание оптимальных схем сотрудничества и взаимодействия;
- укрепление доверия между партнерами и коллегами и пр.

Сводная «карта» европейских киберучений представлена на рис. 4.

По данным ENISA, из 31 страны ЕС и Европей-

Рис. 4. *Сводная карта европейских киберучениях*

ской ассоциации свободной торговли (*EACT*) 6 провели собственные национальные киберучения три раза, 4 – два раза и 12 – один раз. При этом Кипр, Мальта, Люксембург и Чехия еще не проводили собственных национальных киберучений, но приняли выборочное участие в ряде международных киберучений. При этом 61 % киберучений были национальными, и 39%– международными. Это свидетельствует о тенденции развития международного сотрудничества в области кибербезопасности ввиду того что масштаб, характер воздействия и последствия современных кибератак не сдерживаются физическими границами отдельно взятой страны.

В 57% киберучениях принимали участие представители государственных и коммерческих организаций и структур, в 41 % – только государственных организаций (рис. 5).

И только одно киберучение было организовано и проведено коммерческой структурой, что свидетельствует о необходимости более активного вовлечения коммерческих организаций в данный процесс. В целом, в ближайшие годы прогнозируется устойчивый рост государственно-коммерческого сотрудничества в области кибербезопасности. Среднее количество участников типового киберучения составило 200 человек.

На рис. 8 представлены возможные типы оценки проведенных киберучений, которые использовались как по отдельности, так и совместно. В частности, в 16 % случаев были использованы итоговые

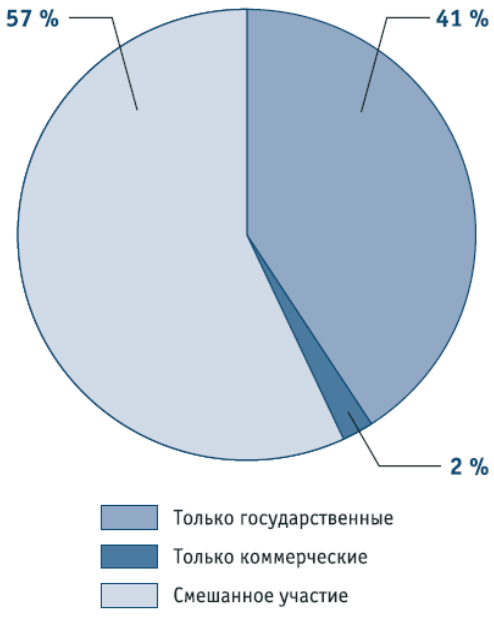

Рис. 5. *Степень участия государственных и коммерческих организаций в киберучениях*

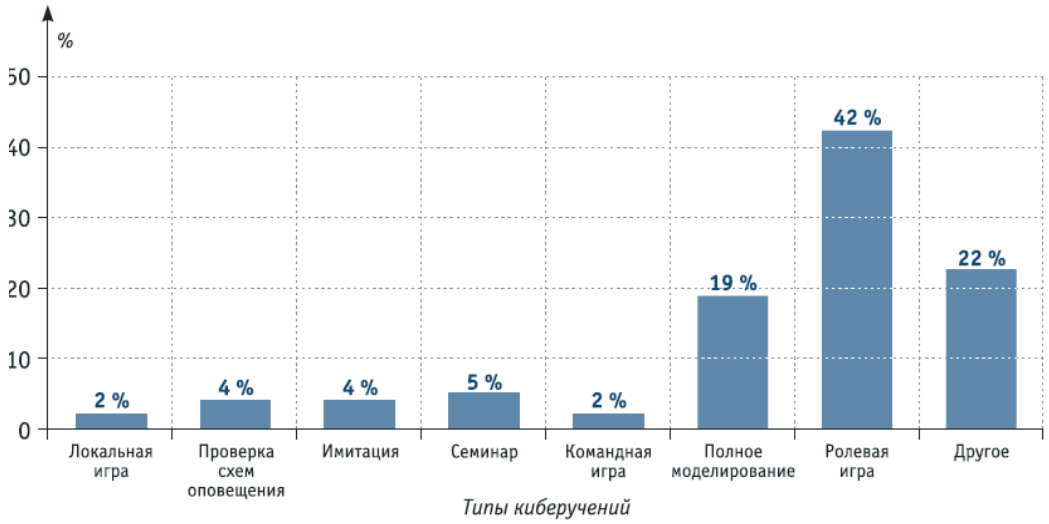

Рис. 6. *Возможные типы киберучений*

семинары, в 31% – итоговые доклады, в 17%– рабочие сессии по недостаткам и замечаниям, в 12% – самооценка участников киберучений (с подготовленными заранее формами самооценки).

Отечественная практика

Следует констатировать, что в настоящее время отечественная практика организации и проведения киберучений только зарождается. Вместе с тем, накоплен значительный положительный опыт проведения учений и тренировок различными отечественными силовыми структурами, например МЧС России [5–7]. Если обобщить известный опыт и переложить его на новую область киберучений, то становится возможным предложить следующие методические указания.

Общие требования

Киберучения должны проводиться в соответствии с требованиями планирующих документов, в отдельных случаях – по указаниям соответствующих должностных лиц. Основными условиями подготовки и проведения киберучений являются:

- всесторонний учет характера возможных последствий информационно-технических воздействий атакующей стороны;

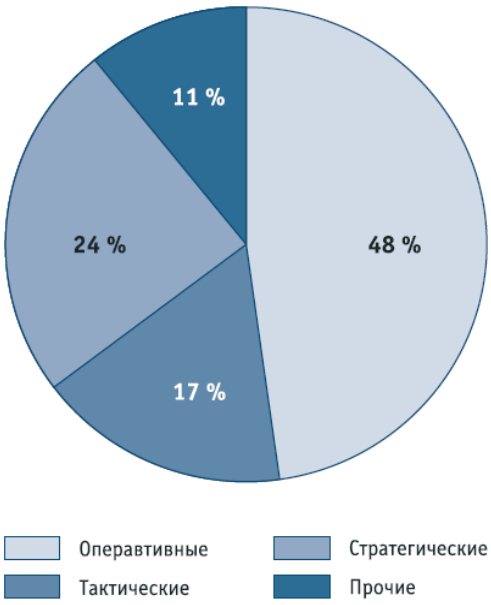

Рис. 7. *Направленность решения задач киберучений*

Рис. 8. *Возможные типы оценки киберучений*

- практический опыт нейтрализации групповых и массовых кибератак.

В ходе киберучений должны отрабатываться мероприятия по обеспечению требуемой устойчивости функционирования критически важных объектов национальной инфраструктуры в условиях информационно-технического воздействия вероятного противника, в том числе:

- приведение служб информационных технологий и информационной безопасности в состояния, оптимальные для своевременного пресечения, выявления и нейтрализации известных и неизвестных ранее кибератак;

- определение оптимальных способов сокращения сроков приведения в различные степени готовности; на критически важные информационные объекты национальной инфраструктуры;

- устранение ранее выявленных недостатков и замечаний.

При проведении киберучений необходимо воспроизвести максимально приближеннуюк реальности ситуацию, имитирующую возможное

- достижение слаженности и согласованности в работе киберкомандования и подчиненных органов управления и формирований;

- оценивание качества соответствующих организационных и технических мер информационной безопасности, проверка правильности и полноты разработанных ранее планов и других нормативных документов по организации и проведению киберучений и пр.

В целом киберучения должны способствовать повышению уровня специальной подготовки руководящего состава и подчиненных органов управления, сил и средств кибербезопасности для надлежащего обеспечения устойчивости функционирования критически важных объектов национальной инфраструктурыв условиях информационно-технических воздействий вероятного противника.

Киберучения можно разделить по своему назначению на плановые, проверочные, показательные и исследовательские, а по уровню проведения – на международные, национальные или федеральные, региональные, муниципальные и объектовые (рис. 9).

Роль руководства

Руководитель киберучения несет полную ответственность за своевременную подготовку и качество проведения учения. Он осуществляет руководство подготовкой и проведением киберучения лично либо через заместителей и штаб руководства киберучениями.

При подготовке киберучения руководитель определяет:

- тему учения;

- **ос**новные этапы;

- состав участников;

- место и время проведения;

- состав руководства подготовкой киберучения.

Он также осуществляет контроль за разработкой необходимых документов для проведения киберучения, в ходе киберучения направляет работу заместителей (помощников), штаба руководства киберучениями, а также обучаемых на достижение поставленных целей киберучения, полную и качественную отработку всех вопросов в соответствии с планом киберучения. Штаб руководства киберучениями является основным органом управления учением, обеспечивающим выполнение всех мероприятий по организации и проведению киберучения. Он разрабатывает соответствующие документы по подготовке и проведению киберучения, осуществляет подготовку посредников, руководящего состава, органов управления и других его участников, пунктов управления, систем связи и оповещения и всестороннего материально-технического обеспечения киберучения.

Разработка документов киберучения

При подготовке киберучения разрабатываются следующие основные документы:

- приказ о подготовке и проведении киберучения;

- календарный план подготовки киберучения;

- схема организации руководства киберучением;

- замысел киберучения;

- организационно-методические указания для привлекаемых формирований по подготовке и проведению киберучения;

- задания, вводные, распоряжения;

- план проведения киберучения;

- план наращивания обстановки;

- план проведения практических мероприятий в ходе киберучения (разрабатывается отдельно для привлекаемых на учение формирований);

- частные планы работы заместителей (помощников) и руководителей формирований и пр.

Представленный перечень возможных документов, разрабатываемых при подготовке киберучения, в зависимости от обстановки может быть сокращен или расширен по решению руководителя учения. Последовательность и конкретные сроки подготовки документов устанавливаются календарным планом подготовки киберучения.

Приказ (распоряжение) о проведении киберучений рекомендуется издать не позднее чем за два месяца до их начала. В нем должны быть определены

- тема киберучения;

- сроки и продолжительность киберучения;

- руководитель, заместители, штаб руководства киберучением;

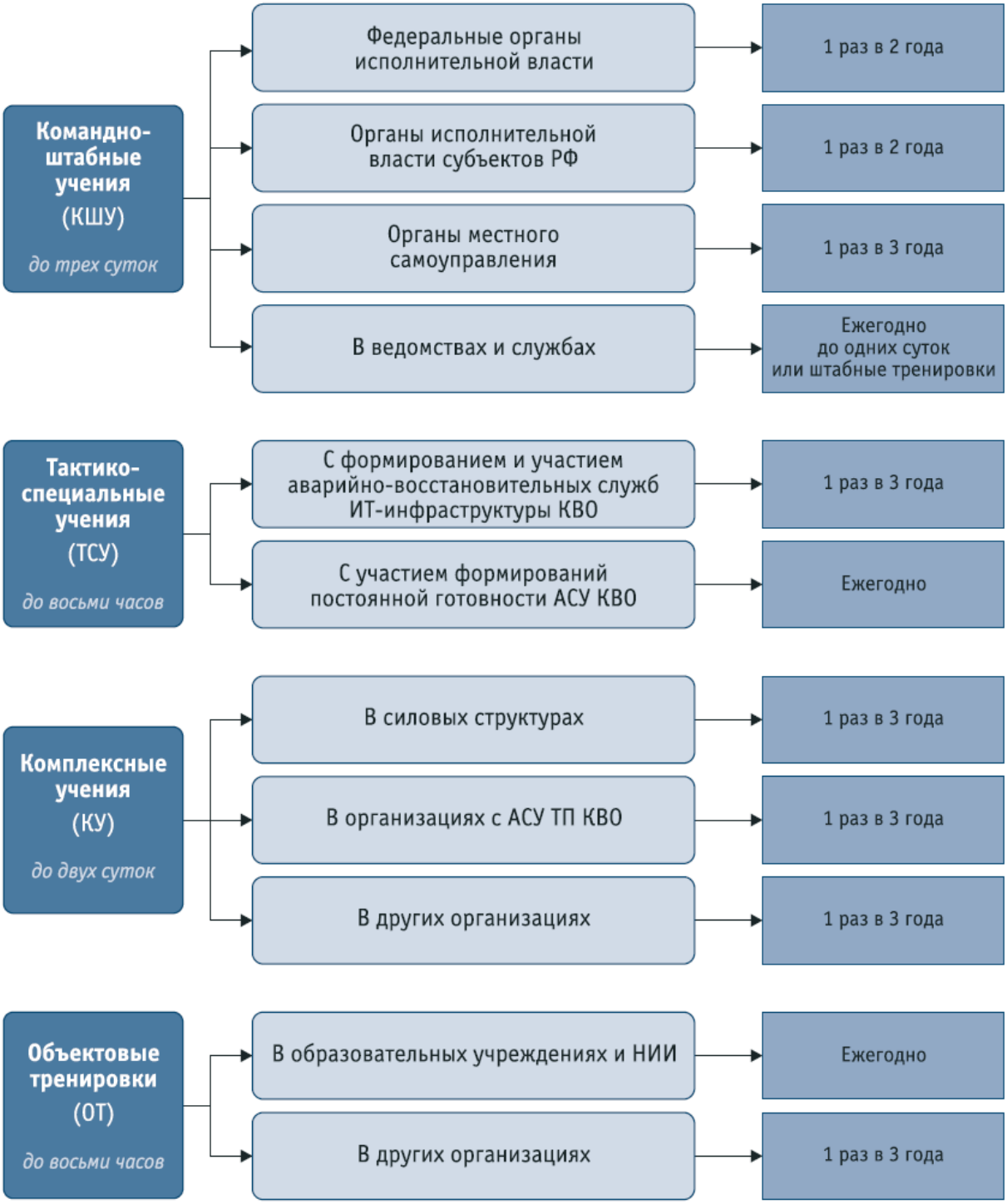

***Рис. 9**. Возможные виды киберучений*

- сроки разработки замысла киберучения и организационных указаний;
- материалы по подготовке к киберучению личного состава, в том числе по соблюдению мер безопасности, материально-техническому обеспечению, порядку представляемых вштаб руководства киберучением докладов;
- другие вопросы, исходя из конкретной обстановки.

Приказ доводится до руководящего состава органов управления, привлекаемых к учению, в части их касающейся.

Календарный план подготовки киберучения является рабочим документом штаба руководства. Он включает в себя основные мероприятия по подготовке учения, очередность и сроки их исполнения, ответственных исполнителей. В разделах плана отражаются:

Таблица

№ п/п	Наименование документа	КШУ	КУ	ТСУ	ТР	Исполнитель
1.	Приказ руководителя организации о проведении киберучения	+	+	+	+	Руководитель службы информационной безопасности
2.	Замысел киберучения с пояснительной запиской	+	–	–	–	Штаб руководства киберучениями
3.	План наращивания обстановки	+	–	–	–	Штаб руководства киберучениями
4.	План практических мероприятий	+	–	–	–	Штаб руководства киберучениями
5.	Организационные указания по подготовке к киберучению – входят в состав приказа о проведении киберучения	+	+	+	+	Штаб руководства киберучениями
6.	Схема организации руководства киберучения	+	+	+	+	Штаб руководства киберучениями
7.	Календарный план подготовки киберучения	+	+	+	+	Штаб руководства киберучениями
8.	План проведения киберучения	+	+	+	+	Штаб руководства киберучениями
9.	График проведения киберучения	+	+	+	–	Штаб руководства киберучениями
10.	Перечень и содержание вводных	+	+	+	+	Штаб руководства киберучениями
11.	План исследований	+	+	+	–	Инженер исследователь в области информационной безопасности
12.	Планы обеспечения устойчивости функционирования КВО в условиях кибератак	+	+	+	–	Заместители руководителя киберучения, начальники служб информационных технологий ИТ и ИБ
13.	Частные планы заместителей руководителя киберучения (помощников, посредников)	+	+	+	+	Заместители, помощники руководителя киберучений, посредники
14.	План рекогносцировки района учения	–	+	+	–	Штаб руководства киберучениями
15.	Инструкция по мерам безопасности	–	+	+	+	Инженер по технике безопасности

- перечень организационных мероприятий по подготовке киберучения;
- сроки разработки учебно-методических документов;
- порядок и сроки подготовки к киберучению руководства, штаба, обучаемых, пунктов управления, систем связи и оповещения;
- меры по материально-техническому обеспечению киберучения;
- порядок контроля за ходом подготовки.

Замысел киберучения разрабатывается текстуально (желательно с приложениями электронной карты или схемы, 3D-модели и спутниковых фотоснимков высокой разрешимости). В нем указывается:

- тема киберучения;
- учебные вопросы и порядок их отработки;
- продолжительность киберучения;
- состав участников;
- организация руководства;

- общая (исходная) и частная обстановка;
- порядок проведения киберучения; его этапы, их наименование, ход, продолжительность;
- отрабатываемые практические мероприятия;
- порядок проведения разбора.

После разработки и утверждения замысла киберучения руководителем штабу руководства необходимо разработать ***организационно-методические указания*** по подготовке и проведению киберучения, которые в срок не позднее 1 месяца до начала мероприятия необходимо довести до соответствующих органов управления, государственных и частных компаний и организаций, привлекаемых к киберучению.

В упомянутых организационно-методических указаниях определяются:
- время проведения киберучения;
- тема киберучения;
- учебные цели;
- состав руководства учением;
- привлекаемые силы и средства;
- перечень формирований, привлекаемых к выполнению практических мероприятий;
- перечень государственных и частных компанийиорганизаций, привлекаемых к киберучению;
- порядок организации управления и связи в ходе учения;
- место размещения штаба руководства и участников;
- мероприятия по подготовке участников;
- другие практические вопросы.

В ***плане проведения*** киберучения указываются:
- тема и цели,
- состав участников,
- время и место его проведения,
- этапы, их продолжительность,
- учебные вопросы,
- создаваемая обстановка (содержание вводных),
- ожидаемые действия,
- работа руководителей.

Подготовка участников киберучения

Подготовка обучаемых представляет собой комплекс мероприятий, имеющий целью обеспечить успешное проведение киберучения, и включает в себя подготовку руководящего состава, органов управления, формирований различной подчиненности, служб информационной безопасности и информационных технологий привлекаемых государственных и коммерческих организаций и структур. Упомянутая подготовка осуществляется заблаговременно на плановых занятиях и течение всего учебного года, а также на дополнительно проводимых занятиях, сборах и тренировках в ходе непосредственной подготовки к киберучению. Подготовка участников (применительно к занимаемым ими должностям) призвана обеспечить полную и качественную отработку всех учебных вопросов и выполнение функциональных обязанностей при обеспечении устойчивости функционирования критически важных объектов национальной инфраструктуры в условиях информационно-технических воздействий противника.

Методика проведения киберучения

Основными методами и содержанием работы должностных лиц руководства и посредников в ходе киберучения являются:
- принятие на вооружение так называемой «лучшей практики» организации и проведения крупномасштабных транснациональных и национальных киберучений;
- формирование и совершенствование личного опыта проведения киберучений;
- личное изучение стиля и методов работы обучаемых в ходе учения;
- заслушивание кратких докладов обучаемых;
- изучение отработанных документов;
- проверка качества и эффективности выполняемых на учении практических мероприятий;
- оказание помощи обучаемым в выполнении функциональных обязанностей;
- обобщение опыта работы и объективная информация о положительных результатах или недостатках, выявленных в ходе киберучений;
- формирование и сопровождение актуального банка организационно-распорядительных документов, методического и научного сопровождения киберучений и пр.

Целесообразно проведение киберучений с максимальной практической направленностью, когда при отработке конкретных задач обучаемые демонстрируют не только теоретические знания, но и практические навыки с использованием соответствующих технических средств обеспечения устойчивости критически важных объектов в условиях информационно-технических воздействий, а также способность оперативно принимать правильные решения и взаимодействовать с коллегами в условиях меняющейся оперативной обстановки.

Примерный алгоритм киберучения:
- оповещение и сбор участников учений;
- инструктаж по мерам безопасности;
- проверка технической готовности критически важного объекта к отражению реальных и сымитированных (смоделированных) кибератак;
- доведение заданий (вводных) до руководителей формирований;
- оценка обстановки и принятие решения руководителями формирований и привлекаемых государственных и коммерческих организаций;
- организация и поддержание устойчивой связи

между всеми участниками;

- практические действия органов управления, формирований и привлекаемых государственных и коммерческих организаций по вводным;
- наращивание обстановки (новые вводные);
- практические действия с учетом изменения обстановки, осуществление маневра силами и средствами, организация взаимодействия между формированиями;
- своевременность и полнота докладов;
- оценка степени выполнения поставленных задач.

Разбор киберучения

Разбор является важной заключительной частью киберучений и имеет большое учебно-воспитательное значение. Цель разбора состоит в том, чтобы на основе требований нормативных документов, а также всестороннего анализа работы и действий обучаемых подвести итоги киберучения и определить – в какой степени достигнуты поставленные учебные цели, какие выводы необходимо сделать для устранения выявленных недочетов и дальнейшего повышения готовности критически важных объектов национальной инфраструктуры к пресечению, обнаружению и своевременному подавлению массовых и групповых кибератак.

Заключение

В едином пространстве стран Содружества Независимых Государств (СНГ) вопросам информационной безопасности уделяется достаточно много внимания. Так, в октябре 2008 года Решением Совета глав государств Содружества была утверждена *Концепция сотрудничества государств-участников СНГ в сфере обеспечения информационной безопасности*. В ходе минского (октябрь 2013 года) саммита глав государств СНГ была одобрена *Концепция сотрудничества государств-участников СНГ в борьбе с преступлениями, совершаемыми с использованием информационных технологий*. На заседании Совета глав правительств СНГ 20 ноября 2013 года в Санкт-Петербурге было принято *Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в области обеспечения информационной безопасности*.

25 декабря 2013 года Республика Беларусь и Российская Федерация подписали двухстороннее межправительственное Соглашение о сотрудничестве в области обеспечения международной информационной безопасности. Прорабатывается вопрос о создании *Единого Центра по обеспечению безопасности в киберпространстве государств-участников СНГ*.

В Российской Федерации в Государственной программе «Информационное общество (2011–2020 годы)» выделен ряд приоритетов развития в области информационной безопасности:

1) противодействие использованию потенциала информационных технологий в целях угрозы национальным интересам Российской Федерации;

2) обеспечение технологической независимости Российской Федерации в отрасли информационных технологий;

3) развитие технологий защиты информации, обеспечивающих неприкосновенность частной жизни, личной и семейной тайны, а также безопасность информации ограниченного доступа;

4) обеспечение развития законодательства Российской Федерации и совершенствование правоприменительной практики в сфере информационных технологий.

В целевой программе «Обеспечение безопасности автоматизированных систем управления производственными и технологическими процессами (АСУ ТП) критически важных объектов (КВО) инфраструктуры Российской Федерации» определены следующие актуальные задачи:

- проведение комплекса мероприятий по развитию систем, средств и методов технической оценки уровня реальной защищенности автоматизированных систем управления (АСУ) КВО и критической информационной инфраструктуры в целом;
- создание единых реестров программных и аппаратных средств, используемых в автоматизированных системах управления КВО, создание баз данных, касающихся надежности функционирования АСУ КВО, состояния их защищенности, состояния технического оборудования, оценки эффективности действующих и внедряемых на критически важных объектах мер безопасности;
- проведение комплекса организационно-технических мероприятий по исключению прохождения информационного обмена автоматизированных систем управления КВО по территориям иностранных государств, а при технической невозможности такого исключения – создание и применение защитных мер, обеспечивающих отсутствие любых негативных воздействий на процессы, контролируемые автоматизированными системами управления КВО, в случае нарушения штатного функционирования этого канала связи;
- разработка комплекса мер по созданию и внедрению телекоммуникационного оборудования, устойчивого к компьютерным атакам;
- создание хранилища эталонного программного обеспечения, используемого в автоматизированных системах управления КВО и на других объектах критической информационной инфраструктуры;
- развитие (с учетом мобилизационной готовности) научно-производственной базы, обеспечивающей выпуск систем (средств) обеспечения безо-

пасности автоматизированных систем управления КВО и иных объектов критической информационной инфраструктуры;

- разработка и внедрение импортозамещающих технологий, материалов, комплектующих и других видов продукции, используемых в автоматизированных системах управления КВО.

Также в упомянутой целевой программе поставлены следующие поисковые и научные задачи (в рамках НИОКР):

- разработка методов и средств своевременного выявления угроз и оценки их опасности для автоматизированных систем управления КВО и иных элементов критической информационной инфраструктуры;

- разработка и внедрение специализированных информационно-аналитических систем, развитие исследований в области математического моделирования процессов обеспечения безопасности автоматизированных систем управления КВО и иных объектов критической информационной инфраструктуры, направленных на выработку вероятных сценариев развития ситуации и поддержку управленческих решений;

- разработка и внедрение комплексных систем защиты и обеспечения безопасности автоматизированных систем управления КВО и иных объектов критической информационной инфраструктуры, отвечающих современному уровню развития информационных технологий и минимизирующих участие обслуживающего персонала в настройке и эксплуатации входящих в их состав программно-аппаратных средств;

- разработка для автоматизированных систем управления КВО специализированных экономически целесообразных информационных технологий, исключающих или в максимальной степени снижающих на технологическом уровне обмен информацией, подлежащей обязательной защите.

Вместе с тем проведенный сравнительный анализ поставленных задач с аналогичными задачами *Цифровой повестки дня для Европы* и рядом специальных *Сообщений Европейской Комиссии* свидетельствует о необходимости оперативной проработки вопросов организациии проведения киберучений и обсуждения соответствующих вопросов не только на государственном и межведомственном, но и на международном уровнях взаимодействия (врезка 3).

Для этого целесообразно воспользоваться накопленным передовым опытом Евросоюза, в частности ENISA, а также учесть положительный опыт проведения киберучений соответствующими отечественными силовыми структурами.

Литература (References):

1. Евросоюз и США проводят совместные киберучения [Электронный ресурс]. – Режимдоступа: http://www.itsec.ru/newstext.php?news_id=81407 (07.11.2011).
2. Общее пространство внутренней безопасности в ЕС: политические аспекты. / Отв.ред. – С. В. Уткин. – М.: ИМЭМО РАН, 2011. – 146 с.
3. Смирнов А. А. Обеспечение информационной безопасности в условиях виртуализации общества: опыт Европейского Союза. Монография. – М.: ЮНИТИ-ДАНА, 2011. – 196 с.
4. Фред Шрайер, Барбара Викс, Теодор Ч. Винклер. Кибербезопасность: дорога, которую предстоит найти. – Женева: Женевский центр демократического контроля над вооруженными силами, 2013. – 196 с.
5. Федеральный закон РФ от 21.12.94 № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера».
6. Постановление Правительства РФ от 30.12.03 № 794 «О единой государственной системе предупреждения и ликвидации чрезвычайных ситуаций».
7. Постановление Правительства РФ от 04.09.03 № 547 «О подготовке населения в области защиты от чрезвычайных ситуаций природного и техногенного характера».
8. European Data Protection Supervisor [Электронный ресурс]. – Режим доступа:http://www.edps.europa.eu/EDPSWEB/edps/cache/off/pid/1.
9. Network and Information Security: Proposal for A European Policy Approach. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. Brussels, 6.6.2001 [Электронный ресурс]. – Режим доступа: http://eurlex.europa.eu/LexUriServ/site/en/com/2001/com2001_0298en01.pdf.
10. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March2004 establishing the European Network and Information Security Agency.
11. A strategy for a Secure Information Society – Dialogue, partnership and empowerment. Communication from the Commission to the Council, the European Parliament, the European economic and social Committee and the Committee of the Regions. Brussels, 2006 [Электронный ресурс]. – Режим доступа: http://ec.europa.eu/information_society/doc/com2006251.pdf.
12. Communication from the Commission to the European Parliament and the Council «The EU Internal Security Strategy in Action: Five steps towards a more secure Europe». Brussels, 22.11.2010. COM(2010).