ПЕРСПЕКТИВНЫЕ МЕТОДЫ АНАЛИЗА ИНФОРМАЦИОННЫХ ПОТОКОВ В СФЕРЕ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ МЧС РОССИИ (ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЙ ОБЗОР – ЧАСТЬ 1)

А.С. Артамонов, кандидат физико-математических наук, профессор.
ООО «Биоклимат», г. Новосибирск.
А.Ю. Иванов, доктор технических наук, профессор.
Санкт-Петербургский университет ГПС МЧС России

Обоснована целесообразность использования новых подходов к обеспечению информационной безопасности автоматизированных систем МЧС России. Исследованы возможности применения перспективных методов обработки данных о деструктивных информационных воздействиях на указанные системы и противодействии им.

Ключевые слова: системный подход, аналитика больших данных, поведенческий анализ, экспертный анализ сетевой активности, когнитивная аналитика

ADVANCED METHODS OF ANALYSIS OF INFORMATION FLOWS IN THE SPHERE OF SECURITY OF THE AUTOMATED SYSTEMS OF EMERCOM OF RUSSIA (INFORMATION-ANALYTICAL REVIEW – PART 1)

A.S. Artamonov. Bioclimate Company Ltd, Novosibirsk.
A.Yu. Ivanov. Saint-Petersburg university of State fire service of EMERCOM of Russia

In the article the expedience of the use of new approaches to information security of the automated systems of EMERCOM of Russia. Researched the possibilities of application of the promising methods for processing data about destructive information influences on these systems and counteract them.

Keywords: systemic approach, big data analytics, behavioral analysis, expert analysis of the network activity, cognitive intelligence

Характер применения сил и средств МЧС России при проведении операций в зонах чрезвычайных ситуаций (ЧС) требует постоянного повышения уровня оперативности и обоснованности решений, принимаемых должностными лицами всех уровней. В современных условиях реализация этого требования невозможна без активного и всестороннего использования автоматизированных систем. Поэтому автоматизацией охвачены различные структуры, задействованные в процессе предупреждения, устранения и ликвидации последствий ЧС, такие как Единая государственная система предупреждения и ликвидации чрезвычайных ситуаций (РСЧС), Национальный центр управления в кризисных ситуациях (НЦУКС) и др. Тем не менее расширение масштаба автоматизированных систем, обеспечивающих деятельность названных структур (Автоматизированная информационно-управляющая система (АИУС) РСЧС и Автоматизированная система (АС) НЦУКС), не может не поставить ряд проблем перед их разработчиками и лицами, ответственными за применение. К их числу относится проблема обеспечения информационной безопасности.

Многолетняя практика противодействия информационным угрозам показывает, что адекватное реагирование на попытки дестабилизации работы автоматизированных систем

требует всестороннего и скрупулезного анализа предполагаемых шагов атакующей стороны. Значимость этого этапа постоянно возрастает, поскольку действия нарушителей информационной безопасности становятся все более изощренными и тщательно маскируемыми. Сложившееся положение требует реализации технологии распознавания деструктивных воздействий на основе новых методов анализа информационных потоков, позволяющих осуществлять оценку воздействий на АС.

Ландшафт пространства киберугроз

Информационные атаки сегодня стали неотъемлемой частью повседневной жизни. Государственные организации, частные лица, коммерческие и некоммерческие предприятия, благотворительные фонды систематически подвергаются информационным нападениям. При этом объем и изощренность атак непрерывно увеличиваются. Проблема кибербезопасности стала одной из самых острых, поскольку информация – это один из самых ценных ресурсов, и она всегда являлась главной целью хакеров. Как правило, преступники охотятся за информацией, способной повысить их денежный доход. Сюда относятся финансовая, деловая и техническая информация, интеллектуальная собственность, персональные сведения.

Отмечается, что в 2014 г. 70 % случаев утечки информации приходилось на хищение персональных данных, что связано с относительной доступностью, легкостью и низкими рисками конвертации этой информации в реальные деньги [1]. Примеры атак на персональные данные приведены в таблице [2, 3].

За 2014 г. в России зафиксировано 43 тыс. киберпреступлений. Если учесть, что от 35 % до 70 % атак остаются необнаруженными [1, 4], этот показатель можно считать сильно заниженным. В июне 2016 г. Сбербанк России оценил потери экономики страны в 600 млрд руб. [5]. В целом экономические последствия кибернетических преступлений по всему миру составляют от 300 млрд до 1 трлн дол. США, то есть от 0,4 % до 1,4 % мирового ВВП [6].

Таблица. **Примеры атак на персональные данные**

Дата	Характер инцидента
Август 2014 г.	Хакеры получили доступ к данным пяти крупных банков США и Европы, в том числе *JPMorgan Chase*. ФБР бездоказательно обвинило в этом российских хакеров
Октябрь 2014 г.	*Staples*, *Inc*. (крупная американская компания по продаже офисного оборудования) объявила, что хакеры получили доступ к транзакциям 1,2 млн покупателей в 115 офисах компании
Октябрь 2014 г.	Департамент занятости штата Орегон (США) обнаружил взлом базы персональных данных, содержащей информацию о более 850 тыс. клиентов
Ноябрь 2014 г.	Почтовая служба США выявила взлом базы персональных данных на 800 тыс. сотрудников
Февраль 2015 г.	*Anthem Inc*. (одна из крупнейших американских страховых компаний) подверглась изощренной кибератаке, которая привела к утечке персональной информации о более 80 млн клиентов
Май 2016 г.	Специализирующаяся на кибербезопасности компания *Hold Securities* обнаружила один из крупнейших в истории архивов с украденными личными данными, в котором содержатся сведения о 272 млн аккаунтов на сервисах *Mail.ru*, *Gmail*, *Yahoo* и *Microsoft*

Большинство угроз может быть отнесено к одной из следующих категорий [7]:
– целенаправленные устойчивые угрозы (*Advanced Persistent Threat*, *APT*);
– распределенные атаки «отказ в обслуживании»;
– внедрение вредоносных программ, включая вирусы и рекламные заставки;
– инсайдерские угрозы;

– фишинг, спуфинг и другие формы мошенничества с использованием электронной почты;

– социальная инженерия и другие формы психологической манипуляции;

– внедрение кодов (*SQL*, *NoSQL*, *OS command injection*);

– перенаправление/изменение, манипулирование *URL*;

– атаки нулевого дня (*Zero-Day Attacks*).

Пространство кибернетического противостояния быстро эволюционирует. Разнообразие угроз растет, а вектор атак смещается в сторону изощренных методов. На смену вредоносным программам, которые можно остановить на периферии защищаемой системы, приходят целенаправленные устойчивые угрозы (*APT*), которые медленно двигаются к намеченной цели, адаптируясь к атакуемой среде. В результате таких атак могут быть не только похищены ценные данные, но и выведены из строя промышленные объекты, энергетические системы, системы жизнеобеспечения различного уровня, вплоть до государственного.

Методы и средства атак прогрессируют с развитием новых технологий. Везде, где повышается уровень компьютеризации и объем использования данных, растут информационные риски. Наблюдается всплеск новых угроз в области социальных сетей, мобильных устройств, а также частных, публичных и гибридных облачных технологий.

Киберпреступники становятся все более изобретательными и оснащенными современными технологическими средствами. Это команды профессионалов, хорошо разбирающихся в средствах нападения и защиты. В их распоряжении находятся финансы, средства тестирования новых типов атак, собственные исследовательские группы. Такой бизнес приносит колоссальные доходы.

По оценкам экспертов Всемирного экономического форума (*Davos Summit*) кибератаки вошли в список главных глобальных рисков десятилетия [8]. Эксперты полагают, что эти атаки существенно замедляют темпы развития технологий и бизнес-инноваций. Однако существует и положительный аспект постоянной эволюции ландшафта киберугроз – стимуляция развития новых, передовых средств обеспечения информационной безопасности.

Проблема информационной безопасности возрастает до уровня национальной безопасности. В июне 2016 г. Совет безопасности Российской Федерации разместил на своем сайте проект новой редакции Доктрины информационной безопасности [9]. Авторы Доктрины выделяют пять блоков угроз национальной безопасности страны в информационной сфере:

– угроза воздействия на критическую информационную инфраструктуру Российской Федерации (электросети, системы управления транспортом и т.п.) и техническую разведку в отношении российских госорганов, научных организаций и предприятий оборонно-промышленного комплекса;

– угроза подрыва суверенитета и территориальной целостности других стран и дестабилизации внутриполитической и социальной ситуации;

– угроза компьютерной преступности, прежде всего в кредитно-финансовой сфере, и увеличение числа инцидентов, связанных с нарушением законных прав граждан на неприкосновенность частной жизни;

– угроза отставания Российской Федерации от ведущих зарубежных государств в создании конкурентоспособных информациионно-коммуникационных технологий и продукции на их основе, что обусловливает зависимость страны от экспортной политики других государств;

– угроза, вызванная стремлением отдельных государств использовать для достижения экономического и геополитического преимущества технологическое доминирование в глобальном информационном пространстве.

Интересно отметить, что если в Доктрине 2000 г. наиболее часто упоминавшимся объектом защиты были «конституционные права и свободы человека» (это словосочетание встречалось в тексте 17 раз), то в новой версии документа этот термин упоминается лишь

трижды. Произошел существенный сдвиг в понимании информационной безопасности страны как безопасности в пространстве информационного противостояния ведущих мировых держав и их союзников. И не случайно, что сегодня НАТО рассматривает киберпространство как еще одну сферу влияния и новое пространство ведения боевых действий наравне с морем, воздухом и сушей [10].

Существующие технологии обеспечения информационной безопасности и их недостатки

До недавнего времени при разработке систем информационной безопасности организации фокусировались в основном на начальной стадии кибератак, то есть на охране периметра защищаемой системы, стремясь предотвратить проникновение вредоносных программам или блокировать подозрительные *IP*- адреса и *URL*. Такой подход ориентирован на борьбу с прямолинейными одноходовыми кибератаками, но не способен обеспечить защиту от целенаправленных устойчивых угроз, которые ведут многошаговые, разветвленные и распределенные во времени атаки.

Безусловно, контроль безопасности и защита наиболее уязвимых элементов по-прежнему важны, однако, выстраивая систему защиты, организации должны исходить из того, что нарушитель находится внутри информационной системы. Учитывая этот факт, наряду с мероприятиями по предотвращению кибератак необходимо развивать и внедрять методы и средства обнаружения и пресечения действий преступников в защищаемой системе и ликвидации их последствий. Эта деятельность должна быть основана на анализе всех активностей внутри информационной инфраструктуры.

Большинство организаций сегодня не готово противостоять кибернетическим атакам. Недавний опрос, проведенный компанией *ESG* (*Enterprise Strategy Group*), выявил следующие слабые стороны в обеспечении информационной безопасности: недостаточный причинно-следственный анализ и анализ последствий кибератак, отсутствие необходимых данных и аналитических подходов, отсутствие ретроспективного анализа и оперативной адаптации системы защиты для предотвращения подобных атак в будущем [2]. Специалисты компании *SAS* – одного из лидеров в области аналитики – считают, что новыми вызовами в сфере информационного противоборства являются следующие [11]:

– высокие темпы развития информационных технологий;

– управление большими массивами данных;

– необходимость быстрой обработки данных о кибератаках;

– анализ и модернизация системы защиты на основании новых сведений;

– большое количество сообщений, генерируемых системой защиты и требующих оперативной реакции;

– растущее разнообразие кибернетических угроз.

К наиболее популярным технологиям противодействия кибернетическим угрозам, используемым в настоящее время, можно отнести следующие:

– системы обнаружения вторжений (*Intrusion Detection System*, *IDS*). Задача этих систем – информировать администратора о возможных нарушениях для того, чтобы он предпринял определенные действия для их предотвращения;

– системы противодействия вторжениям (*Intrusion Prevention System*, *IPS*), отслеживающие трафик активности и способные обнаруживать и блокировать потенциальные опасности;

– системы управления информацией о безопасности и текущих событиях (*Security Information and Event Management*, *SIEM*). Они делятся на два класса: системы управления информацией о безопасности (*Security Information Management*, *SIM*), используемые для анализа данных, и системы управления текущими событиями (*Security Event Management*, *SEM*), обрабатывающие данные в реальном времени и способные обнаруживать вторжения.

Технологии *IDS* и *IPS* не способны адекватно реагировать на новые киберугрозы, так как они основаны на исполнении определенного набора правил, которые технически и организационно невозможно обновлять непрерывно.

SIEM-системы представляют собой следующую волну технологических инноваций, нацеленных на обеспечение большей прозрачности в понимании процессов, происходящих в информационной среде. Эти системы были и остаются центральным звеном мониторинга информационной безопасности для большинства крупных организаций, однако и они не в состоянии полноценно противодействовать информационным угрозам.

Эксперты выделяют следующие основные проблемы при работе с *SIEM* [2]:

– анализ корреляций событий в *SIEM*-системах основан на предопределенных схемах и оптимален для идентификации возможных нарушений. Однако он менее эффективен при решении конкретной задачи, не предназначенной для какого-либо обобщения или адаптации для других целей;

– *SIEM*-технологии используют фиксированные схемы хранения данных и поэтому требуют, чтобы данные были соответствующим образом структурированы и форматированы перед тем, как быть загруженными в систему. Это существенным образом ограничивает объемы и типы данных, которые могут быть использованы для анализа и принятия решений, а также требует существенных затрат времени для конечного пользователя на технологическую поддержку системы;

– *SIEM*-технологии основаны на предопределенном контексте, как правило, исполненном в формате реляционных баз данных, означающее, что добавление нового содержания (например, идентификационных данных, географических координат и т.д.) должно быть заранее определено и требует трудозатрат;

– *SIEM*-технологии не обладают необходимой гибкостью и требуют существенной модификации при использовании их конкретным клиентом в определенных условиях: настройка правил вычисления корреляций между событиями, редактирование существующих и создание новых форм отчетов, сопряжение с новыми базами данных и новыми источниками информации и т.д.

Ряд других проблем, отмеченных участниками опроса, – это высокие профессиональные требования к знаниям и навыкам пользователей системы, трудности ее освоения, большое количество ложных извещений, хранение больших объемов информации.

Новые концепции и подходы к проблеме информационной безопасности

В настоящее время недостаточно одних тактических средств, основанных даже на самых современных технологиях борьбы с информационными угрозами, и требуются новые стратегические подходы и концепции.

Системный подход. В условиях, характеризующихся значительным уровнем сложности, многокомпонентностью и непрерывными изменениями, обеспечение информационной безопасности необходимо осуществлять с системных позиций. Неизбежность усложнения систем информационной безопасности связана с возрастающей сложностью, как их внутренней организации, так и внешней среды. Очевидно, что сложность и разнообразие систем защиты не могут уступать системам нападения. Это вытекает из закона о требуемом многообразии [12].

Системный подход можно представить как анализ сети взаимоотношений и взаимодействий между отдельными компонентами сложной системы. Это позволяет разработать общее понимание, терминологию и, самое главное, общий вектор целей. Не секрет, что понимание информационной безопасности администратором безопасности, системным администратором, руководителями подразделений и предприятия не совпадает, а порой полярно.

Еще одна проблема, которую позволяет решить системный подход – это организация сбалансированной информационной безопасности: снижение информационных рисков в одних подразделениях не должно приводить к их росту в других.

Существуют модели управления информационной безопасностью, направленные на формирование целостного подхода к этой проблеме. Основным недостатком многих из них является отсутствие взаимодействия культуры информационной безопасности с ценностями самой организации. Одна из моделей, призванная преодолеть данный недостаток, предложена Лэри Кейли (*Laree Kiely*) и Терри Бензелом (*Terry Benzel*) [13].

Модель включает в себя четыре основные элемента (рис. 1): структуру и стратегию организации, персонал, процесс и технологию, а также шесть динамических связей, описывающих взаимодействие между этими элементами: управление организацией, управление культурой, согласование процесса и технологии, управление непредвиденными ситуациями, человеческий фактор, архитектура информационной безопасности.

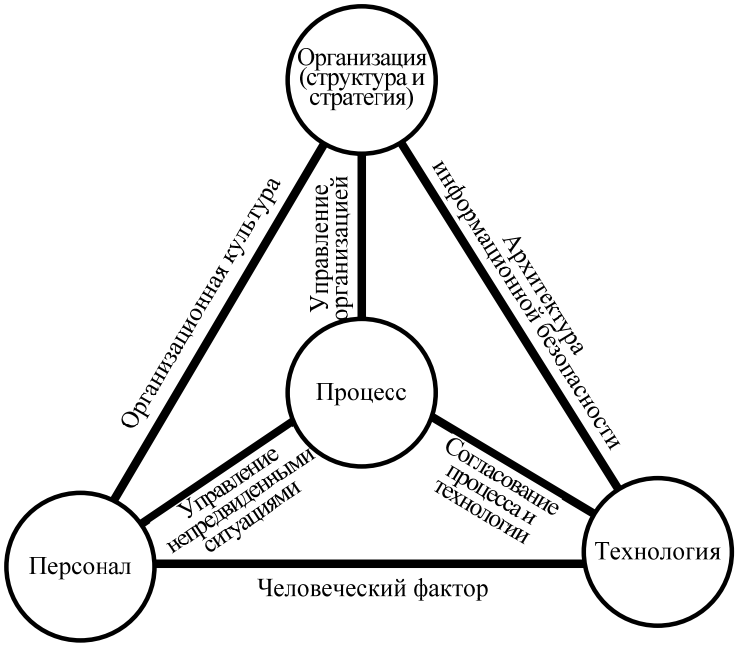

Рис. 1. **Системная модель информационной безопасности**

Модель предоставляет следующие возможности в решении задач зашиты информации: снижение издержек, ликвидация дублирования, лучшее понимание информационных рисков, улучшение сотрудничества между подразделениями, внедрение в сознание управляющего персонала и рядовых сотрудников культуры информационной безопасности. Использование этой модели также позволяет эффективно реагировать на текущие и возможные проблемы, вызванные технологическим прогрессом, глобализацией, организационными преобразованиями, конкуренцией, изменяющимся ландшафтом киберугроз и т.д.

Несомненным достоинством модели является ее гибкость и адаптивность. Она может быть дополнена другими элементами, например, аналитической компонентой (модели, критерии, алгоритмы), а также внешними угрозами и внешними факторами, влияющими на персонал, технологию и организацию.

Аналитика больших данных (Big Data Analytics)

Сегодня аналитика больших данных упоминается как возможный следующий шаг в развитии средств обеспечения информационной безопасности. Переход к новым технологиям хранения и массово-параллельной обработки данных позволяет значительно

увеличить объем анализируемых событий для выявления инцидентов. Большие данные – это совокупность подходов, инструментов и методов высокоскоростной обработки огромных объемов структурированных и неструктурированных данных, разнообразных по содержанию и форме.

Начало эпохи больших данных можно отнести середине 90-х гг. прошлого столетия. Для эволюции больших данных потребовалось всего 20 лет (рис. 2).

Рис. 2. **Эволюция больших данных**

В качестве определяющих характеристик больших данных называют четыре (чаще первых три) *V*:

– объем (*Volume*) – долговременное хранение огромных объемов информации;

– скорость (*Velocity*) – анализ в режиме, близком к реальному времени, благодаря параллельной (распределенной) обработке данных;

– разнообразие (*Variety*) – отсутствие жестких требований к формату и структуре данных;

– ценность (*Value*) – полезность данных для решения функциональных задач.

Технологию больших данных можно разделить на две группы: пакетная обработка (*batch processing*) для терабайтных и более объемов информации, требующая относительно длительного времени, и обработка потока данных (*stream processing*) – для меньших объемов и более коротких временных интервалов.

В настоящее время наиболее популярной технологией пакетной обработки является *Hadoop*, которая предлагает распределенную систему хранения больших файлов (*HDFS*) и программный продукт *MapReduce* для параллельной/распределенной обработки. Имеется ряд специализированных баз данных, таких как *Cassandra*, *CouchDB*, *Greenplum*, *HBase*, *MongoDB* и *Vertica*, а также программных продуктов и платформ для выполнения сложных запросов, анализа и построения моделей на основе алгоритмов машинного обучения: *Pig*, *Hive*, *Mahout*, *Rhadood*. В качестве последних разработок можно назвать *Spark* и *H2O*. В частности, *Spark* позволяет существенно повысить эффективность обработки данных (*data mining*) и использования алгоритмов машинного обучения (*machine learning*) за счет рекуррентной обработки в оперативной памяти и многократного доступа к загруженным в память пользовательским данным. *Spark* предоставляет программные интерфейсы для

языков *Java*, *Scala*, *Python* и *R*, что позволяет использовать обширные библиотеки алгоритмов, написанных на этих языках.

Что касается обработки потока данных (*stream processing*), то в настоящее время не существует доминантой технологии подобной *Hadoop*. В качестве примера таких технологий можно назвать *InfoSphere Stream*, *Jubatus* и *Storm*.

В качестве примеров успешного применения больших данных для целей обеспечения защиты информации можно назвать следующие [14]:

– безопасность компьютерных сетей (*network security*): компания *Zions Bancorporation* [15] анонсировала, что применение *Hadoop* технологий и аналитических инструментов типа *Business Intelligence* позволяют обработать массивы данных и осуществить частотный анализ событий в объемах и временных интервалах, недоступных традиционным *SEIM*-системам: месяцы обработки сократились до нескольких десятков минут;

– обработка огромных массивов данных по информационной безопасности на уровне организации (пользовательская активность, сетевая активность, использование программных продуктов и т.д.). Например, организации масштаба *Hewlett-Packard* генерируют порядка 12 млн событий каждую секунду. Обычные аналитические подходы не приемлемы при таких объемах событий, поскольку порождают большое количество ложных сигналов. Компания *Hewlett-Packard* провела успешный эксперимент с 2 млрд *HTPP*-запросов, 1 млрд *ISP*-запросов и 35 млрд инцидентов – данными, полученными от 900 предприятий и организаций по всему миру, продемонстрировав возможность существенного увеличения точности идентификации нарушений информационной безопасности;

– идентификация ботнетов. Проект, выполненный компанией *BotCloud* с использованием *MapReduce* для анализа сетевого трафика представленного 720 млн протоколов между 16 млн серверов, накопленными в течение 23 ч. Время анализа сетевого графа, содержащего 16 млн узлов и 57 млн ребер, было уменьшено в семь раз за счет использования технологии *Hadoop*;

– обнаружение целенаправленных устойчивых угроз (*APT*), включая профилирование пользователей и обнаружение аномалий в их активности при работе с информационной системой. В 2013 г. *RSA* выпустила прототип *APT*-детектора под названием *Beehive*. Название детектора отражает алгоритм детектирования, основанный на множестве одновременно функционирующих сенсоров, которые совместными усилиями обнаруживают *APT* подобно тому, как пчелы (*bees*), выполняющие каждая свою функцию, поддерживают улей (*hive*). Детектор *Beehive* способен обработать данные, состоящие из 1 млрд. протоколов в течение часа и обнаружить *APT*, которые в противном случае прошли бы незамеченными.

Несомненно, аналитика больших данных будет активно внедряться для обеспечения информационной безопасности. Она подразумевает следующее:

– системный подход к обеспечению информационной безопасности;

– культуру работы с данными;

– наличие организационной структуры интеллектуального анализа данных;

– специалистов, способных строить аналитические модели, создавать и поддерживать алгоритмы для анализа данных, эффективно взаимодействовать с другими участниками процесса обеспечения информационной безопасности.

Аналитика больших данных возможна после того, как организация научилась эффективно и полно использовать уже имеющуюся информацию [16, 17]. Говоря о применении больших данных для обеспечения информационной безопасности, необходимо помнить об ограничениях их использования, накладываемых законодательными, юридическими и другими актами: авторские права, право на частную жизнь и т.д.

Литература

1. Фабиано Валлеси. Цифровая атака. URL: http://pbwm.ru/articles/ tsifrovaya-ataka (дата обращения: 23.11.2015).

2. Jon Oltsik, Analytics-based approach to cyber security. May, 2015. URL: https://www.splunk.com/content/dam/splunk2/pdfs/white-papers/esg-solution-showcase-splunk-may-2015.pdf. (дата обращения: 23.11.2015).

3. Reuters: Российские хакеры похитили личные данные 272 млн. пользователей. URL: https://aftershock.news/?q=node/395028. (дата обращения: 04.05.2016).

4. Research: Thwarting sophisticated cyberattacks demand better grasp of big data with more proactive analytics. SAS Global Forum, Dallas, Apr. 27. 2015.

5. Сбербанк оценил потери экономики от кибератак в 600 миллиардов рублей. URL: https://lenta.ru/news/2016/06/10/cyberattack/.(дата обращения: 10.06.2016).

6. McAfee. An Intel Company. Экономические последствия киберпреступности и кибершпионажа. Центр стратегических и международных исследований (CSIS): отчет. 2013.

7. Big Data and Predictive analytic: on the cyber security front line. IDC white paper, February, 2015, IDC #254290.

8. The Global Risks Report 2016 11th Edition. – World Economic Forum. URL: http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf. (дата обращения: 10.06.2016).

9. Доктрина информационной безопасности Российской Федерации: проект. Совет Безопасности Рос. Федерации. URL: http://www.scrf.gov.ru/ documents/6/135.html. (дата обращения: 10.06.2016).

10. Кибервойна только набирает обороты – НАТО вступает в игру. InfoResist. URL: https://inforesist.org/kibervoyna-tolko-nabiraet-oborotyi-nato-vstupaet-v-igru/ (дата обращения: 09.07.2016).

11. SAS: Trends in combating cyber crime Tips and technology for defending your network. URL: http://www.risktech-forum.com/home/search?keywords=cybercrime. (дата обращения: 09.07.2016).

12. Эшби У.Р. Введение в кибернетику. М.: «Иностранная литература», 1959.

13. The business model for information security. URL: https://www.isaca.org/ knowledge-center/bmis/documents/introtobmis.pdf. (дата обращения: 09.07.2016).

14. Cloud Security Alliance (CSA). Big data analytics for security intelligence. URL: https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Big_Data_Analytics_for_Security_Intelligence.pdf. (дата обращения: 09.07.2016).

15. A Case Study In Security Big Data Analysis. 3/9/2012. URL: http://www.darkreading.com/monitoring/a-case-study-in-security-big-data-analys/232602339. (дата обращения: 09.07.2016).

16. Bill Franks. Taming the Big Data Tidal Wave. Finding opportunities in huge data Streams with advanced analytics. John Wiley & Sons, Inc. 2012. 304 p.

17. Big Data Now, Current Perspectives from O'Reilly Media, 2014 Edition.

References

1. Fabiano Vallesi. Tsifrovaya ataka. URL: http://pbwm.ru/articles/ tsifrovaya-ataka (data obrashcheniya: 23.11.2015).

2. Jon Oltsik. Analytics-based approach to cyber security. May. 2015. URL: https://www.splunk.com/content/dam/splunk2/pdfs/white-papers/esg-solution-showcase-splunk-may-2015.pdf. (data obrashcheniya: 23.11.2015).

3. Reuters: Rossiyskiye khakery pokhitili lichnyye dannyye 272 mln. polzovateley. URL: https://aftershock.news/?q=node/395028. (data obrashcheniya: 04.05.2016).

4. Research: Thwarting sophisticated cyberattacks demand better grasp of big data with more proactive analytics. SAS Global Forum. Dallas. Apr. 27. 2015.

5. Sberbank otsenil poteri ekonomiki ot kiberatak v 600 milliardov rubley. URL: https://lenta.ru/news/2016/06/10/cyberattack/.(data obrashcheniya: 10.06.2016).

6. McAfee. An Intel Company. Ekonomicheskiye posledstviya kiberprestupnosti i kibershpionazha. Tsentr strategicheskikh i mezhdunarodnykh issledovaniy (CSIS): otchet. 2013.

7. Big Data and Predictive analytic: on the cyber security front line. IDC white paper. February. 2015. IDC #254290.

8. The Global Risks Report 2016 11th Edition. – World Economic Forum. URL: http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf. (data obrashcheniya: 10.06.2016).

9. Doktrina informatsionnoy bezopasnosti Rossiyskoy Federatsii: proyekt. Sovet Bezopasnosti Ros. Federatsii. URL: http://www.scrf.gov.ru/ documents/6/135.html. (data obrashcheniya: 10.06.2016).

10. Kibervoyna tolko nabirayet oboroty – NATO vstupayet v igru. InfoResist. URL: https://inforesist.org/kibervoyna-tolko-nabiraet-oborotyi-nato-vstupaet-v-igru/ (data obrashcheniya: 09.07.2016).

11. SAS: Trends in combating cyber crime Tips and technology for defending your network. URL: http://www.risktech-forum.com/home/search?keywords=cybercrime. (data obrashcheniya: 09.07.2016).

12. Eshbi U.R. Vvedeniye v kibernetiku. M.: «Inostrannaya literatura». 1959.

13. The business model for information security. URL: https://www.isaca.org/ knowledge-center/bmis/documents/introtobmis.pdf. (data obrashcheniya: 09.07.2016).

14. Cloud Security Alliance (CSA). Big data analytics for security intelligence. URL: https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Big_Data_Analytics_for_Security_Intelligence.pdf. (data obrashcheniya: 09.07.2016).

15. A Case Study In Security Big Data Analysis. 3/9/2012. URL: http://www.darkreading.com/monitoring/a-case-study-in-security-big-data-analys/232602339. (data obrashcheniya: 09.07.2016)

16. Bill Franks. Taming the Big Data Tidal Wave. Finding opportunities in huge data Streams with advanced analytics. John Wiley & Sons. Inc. 2012. 304 p.

17. Big Data Now. Current Perspectives from O'Reilly Media. 2014 Edition.