Национальная система раннего предупреждения о компьютерном нападении

С. А. Петренко, Д. Д. Ступин

под общей редакцией С. Ф. Боева

«Трудное мы делаем сразу,
невозможное требует несколько больше времени»
Академик А.Л. Минц

Содержание

Показано, что задача обеспечения информационной безопасности критической инфраструктуры Российской федерации являются одной из важнейших задач обеспечения суверенитета и обороноспособности государства. Выявлены основные угрозы информационной безопасности Российской Федерации, которые включают в себя угрозы военно-политического, террористического и криминогенного характера. Обоснована необходимость комплексного подхода к обеспечению информационной безопасности не только на национальном, но и на внешнеполитическом уровне. Показано, что известные концепции обеспечения информационной безопасности, исключающие военно-политическое измерение уже неэффективны. Выяснено, что усиление мер противодействия угрозам информационной безопасности в контексте обеспечения национальной безопасности Российской Федерации связано с необходимостью повышения уровня государственного контроля и мониторинга киберпространства. Дана оценка предельным возможностям государственных Ситуационных Центров и ГосСОПКА, а также различных корпоративных Центров мониторинга угроз информационной безопасности (CERT/SCIRT/MSSP/MDR/SOC) для предупреждения компьютерных атак и упреждения перехода критической инфраструктуры Российской Федерации в катастрофические состояния. Показана ключевая роль Киберучений для проверок и оценивания эффективности известных методов и средств обнаружения, предупреждения и нейтрализации последствий компьютерных атак на практике. Обоснована необходимость создания Национальной системы раннего предупреждения о компьютерном нападении на критически важные информационные ресурсы Российской Федерации на основе нано-, био-, инфо- и когнитивных технологий (NBIC-технологий). Обоснована необходимость анализа и обработки сверхбольших объемов структурированной и неструктурированной информации от разнообразных источников Internet/Intranet и IoT/IIoT (тематика Big Data и Big Data Analytics) в реальном масштабе времени для решения поставленной задачи. Приведены возможные концептуальная и математическая постановки задачи.

1.1. Киберпространство как потенциальный источник угроз для критически важных объектов инфраструктуры и информационной инфраструктуры страны в целом
1.2. Концепция доминирования НАТО в киберпространстве. Необходимость обеспечения цифрового суверенитета России
1.3. Киберучения как высшая форма боевой учебы для приобретения навыков и компетенций для решения задач обнаружения, предупреждения и нейтрализации последствий компьютерных атак
1.4. Первые межгосударственные киберучения стран СНГ «Кибер-Антитеррор-2016». Отработка навыков эффективного коллективного противодействия террористическим проявлениям в киберпространстве как на национальном, так и межгосударственном уровне
1.5. Вероятные сценарии проведения компьютерных атак на критически важные сети TCP-IP государства в условиях информационного противоборства
1.6. Примеры вскрытия схем шифрования в беспроводных сетях Wireless LAN семейства IEEE 802.1x
1.7. Вероятные угрозы нарушения конфиденциальности речевой информации в цифровых и IP-УАТС
1.8. Состояние проблемы обнаружения и предупреждения компьютерных атак. Необходимость мониторинга киберпространства
1.9. Возможные постановки задач предупреждения и упреждения, своевременного обнаружения и нейтрализации компьютерных атак

Раздел 2. Предельные возможности известных технологий контроля и мониторинга киберпространства Российской Федерации

Предложен подход к созданию требуемой системы предупреждения на основе так называемого «вычислительного когнитивизма» – сравнительно нового научного направления исследований, в котором познание и когнитивные процессы являются разновидностью символьного вычисления. Показано, что когнитивный подход позволяет создавать системы, принципиально отличающиеся от традиционных систем мониторинга угроз информационной безопасности уникальной способностью к самостоятельному ассоциированию и синтезу новых знаний о качественных характеристиках и количественных закономерностях информационного противоборства. Предложена возможная архитектура Национальной системы раннего предупреждения о компьютерном нападении на информационные ресурсы Российской Федерации на основе конвергентных нано-, био-, инфо-, когнитивных технологий, NBIC- технологий.

2.1. Оценка пригодности ситуационных центров органов государственной власти Российской Федерации для мониторинга угроз информационной безопасности
2.2. Предельные возможности коммерческих операторов услуг безопасности, MSSP/MDR для реагирования на инциденты компьютерной безопасности
23. Возможные способы организации предоставления услуг безопасности для государственных и коммерческих предприятий
2.4. Предельные возможности корпоративных ситуационных центров для реагирования на инциденты безопасности на примере компании Microsoft
2.5. Предельные возможности государственных и корпоративных центров реагирования на инциденты компьютерной безопасности, CERT/CSIRT
2.6. Пример построения ведомственного сегмента системы обнаружения, предупреждения и нейтрализации последствий компьютерных атак (СОПКА) для сети Минобразования Российской Федерации
2.7. Пример разработки программно-аппаратного комплекса иммунной защиты информационных ресурсов национального оператора связи.

Раздел 3. Возможные научно-технические решения проблемы раннего предупреждения о компьютерном нападении на критическую инфраструктуру Российской Федерации

Содержит обзор перспективных технологий CERT и CSIRT, MSSP и MDR, SOC от локальных до глобальных решений, подразумевающих построение разветвленной национальной сети указанных центров. Показаны особенности создания перспективного «облачного» центра реагирования на инциденты безопасности. Рассмотрена задача обеспечения работоспособности перспективных LTE-сетей, так чтобы организация функционирования упомянутых сетей в ходе массовых деструктивных воздействий упреждала приведение к существенным или катастрофическим последствиям. Проведен анализ перспективных научных исследований в области сетевых технологий нового поколения Software defined networking (SDN) или программно-конфигурируемых сетей (ПКС). Предложены конструктивные модели когноморфного и нейроподобного вычислителей, которые отличаются от традиционных на основе архитектуры Фон Неймана и позволяют реализовать упреждающее поведение в ходе информационного противоборства в киберпространстве на основе нового свойства антиципации.

3.1. Типизация эволюционных модификаций «архитектуры фон Неймана» для выбора перспективной аппаратной платформы национальной системы раннего предупреждения о компьютерном нападении
3.2. Создание суперкомпьютерных технологий сверхвысокой производительности для контроля киберпространства Российской Федерации. Проблема организации вычислений эксафлопсной производительности
3.3. Оценка готовности отечественной Программы развития суперкомпьютерных технологий на период до 2025 года для разрешения проблемы раннего предупреждения о компьютерном нападении
3.4. Необходимость и принципиальная возможность создания национальной когнитивной системы раннего предупреждения о компьютерном нападении
3.5. Сбор и обработка больших данных (Big Data) для решения задач предупреждения и упреждения, обнаружения и нейтрализации последствий компьютерных атак
3.6. Возможные методы управления знаниями в условиях информационного противоборства
3.7. Общий подход к задаче создания компьютера будущего. Примеры программ разработки и развития искусственных когнитивных систем, возможность использования технологий «вычислительного когнитивизма» для мониторинга угроз безопасности киберпространства
3.8. Возможные модели и методы для упреждения компьютерного нападения на критически важные информационные ресурсы Российской Федерации

Раздел 4. Перспективные поисковые исследования в области информационной безопасности и раннего предупреждения о компьютерном нападении на критическую инфраструктуру Российской Федерации

Рассмотрены тенденции и перспективы развития Национальной системы раннего обнаружения компьютерного нападения, намечены очередные перспективные задачи для развития упомянутой системы. Подняты вопросы организации программы научно-исследовательских работ в области информационной безопасности. Рассмотрены возможные требования к квалификации конструкторов и инженеров-

исследователей в данной области. Приведен комплексный пример решения задачи раннего обнаружения компьютерного нападения на современные интеллектуальные системы типа Smart Grid.

4.1. Развитие навыков и компетенции инженеров-исследователей и конструкторов для решения технических задач раннего предупреждения о компьютерном нападении
4.2. Проведение перспективных поисковых исследований и разработка прорывных технологий кибербезопасности на примере Агентства перспективных оборонных исследований DARPA США
4.3. Создание сетевых технологий нового поколения для развития национальной системы раннего предупреждения о компьютерном нападении
4.4. Развитие передовых технологий мобильной связи LTE для создания доверенных открытых сегментов национальной системы раннего предупреждения о компьютерном нападении
4.5. Решение задач организации доверенной среды «облачных вычислений» путем контроля и управления процессами обработки данных в виртуальных средах различных уровней конфиденциальности
4.6. Создание перспективных технологий прогнозной аналитики, BI-платформы для визуального представления оперативной информации по результатам мониторинга угроз безопасности
4.7. Создание перспективных технологий мониторинга аномалий функционирования компьютерных систем на примере решений Oracle
4.8. Развитие корпоративных центров оперативного управления ИБ (Security Operations Center – SOC)
4.9. Разработка онтологий кибербезопасности Smart Grid для решения задач раннего предупреждения компьютерного нападения на сети и системы промышленного Интернета, IIoT/IoT
4.10. Развитие стандартов функциональной безопасности и устойчивости функционирования критически важной инфраструктуры Российской Федерации на примере развития ГОСТ Р МЭК 61508

Раздел 5. Заключение. Выводы.

Заключение

Приложение. Перспективная методика обнаружения аномального функционирования компьютерной сети на основе методов размерностей и подобия

1. Анализ подходов и постановка задачи
2. Выявление и анализ новых информативных признаков процесса обнаружения аномального функционирования сети передачи данных
3. Разработка способа обнаружения аномального функционирования сети передачи данных на основе новых информативных признаков
4. Проектирование системы обнаружения аномального функционирования сети передачи данных на основе контроля инвариантов размерности
5. Оценка полученного результата

Об авторах

ПЕТРЕНКО Сергей Анатольевич

Родился в 1968 году в г. Калининград (Балтийский). В 1991 году окончил с отличием Академию имени А.Ф. Можайского по специальности инженер-математик. В 1997 году – адъюнктуру и 2003 году докторантуру Академии имени А.Ф. Можайского. Инженер-исследователь высокой квалификации.

Конструктор систем информационной безопасности критически важных объектов информатизации:

- Трех национальных *Центров мониторинга угроз информационной безопасности и двух* ситуационно-кризисных центров (СКЦ) отечественных Госкорпораций;
- Трех операторов специальных услуг информационной безопасности *MSSP (Managed Security Service Provider)* и *MDR (Managed Detection and Response Services) и д*вух виртуальных доверенных операторов связи MVNO;
- Более 10 Государственных и корпоративных сегментов *Системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (СОПКА) и Системы обнаружения и предупреждения компьютерных атак (СПОКА)* Министерства обороны РФ;
- Пяти центров мониторинга угроз информационной безопасности и реагирования на инциденты информационной безопасности *CERT (Computer Emergency Response Team)* и *CSIRT (Computer Security Incident Response Team) и д*вух индустриальных CERT промышленного Интернет IIoT/IoT;
- Более 20 комплексных систем информационной безопасности IIoT/IoT и экспериментальных полигонов для организации и проведения 10 национальных и 4 международных киберучений на критически важных объектах информатизации. Проектировщик АСУ ТП в защищенном исполнении на уровнях: Level 4 – ERP; Level 3 – MES; Level 2 – SCADA; Level 1 – ПЛК/РЗА; Level 0 – полевые устройства (сегментация, обеспечение отказоустойчивости и доступности, анализ защищенности и контроль целостности, проектирование и внедрение промышленных FW,IDS/IPS, маршрутизаторов и коммутаторов (Modbus, OPC, МЭК 104), антивирусная защита, криптографическая защита информации, контроль изменений, управление киберинцидентами CERT АСУ ТП).

Руководитель государственной научной школы «Математическое и программное обеспечение критически важных объектов РФ».

Эксперт секции по проблемам информационной безопасности научного совета при Совете Безопасности Российской Федерации.

Научный редактор журнала «Инсайд. Защита информации» (входит в перечень ВАК Российской Федерации).

Доктор технических наук, профессор.

Входит **в состав управления**: Межрегиональной общественной организации Ассоциация руководителей служб информационной безопасности **(**АРСИБ), независимой некоммерческой организации Российский Союз ИТ-Директоров (СоДИТ).

Автор и соавтор 8 монографий и более 200 статей по вопросам информационной безопасности (*Труды ИСА и СПИИ Российской Академии Наук, журналы «Вопросы кибербезопасности», «Проблемы информационной безопасности», «Открытые системы», «Инсайд. Защита информации», «Системы безопасности», «Электроника», «Вестник связи», «Сетевой журнал», «Мир Связи Connect» и др.*). В том числе, монографии и практические

пособия издательств «Питер», «Новая Афина» и «ДМК-Пресс»: *«Методы защиты информации в Интернет», «Методы и технологии защиты информации критически важных объектов национальной инфраструктуры», «Методы и технологии облачной безопасности», «Аудит безопасности корпоративных систем Интернет/Интернет», «Управление информационными рисками», «Политики информационной безопасности» и пр.*

Удостоен **премии** «Большой ЗУБР» и «Золотой ЗУБР» в 2014 году за национальные проекты Российской Федерации в области информационной безопасности.

СТУПИН Дмитрий Дмитриевич

Заместитель генерального конструктора ОАО «РТИ».

Родился 25 июля 1955 года в г. Печора. В 1978 году закончил Московский физико-технический институт по специальности «Автоматика и электроника».

В 2001 году защитил диссертацию. В 1978 - 2002 гг. работал в ОАО «Радиотехнический институт имени академика А.Л. Минца». Прошел путь от инженера до первого заместителя генерального директора.

С 2002г. - заместитель генерального директора - руководитель комплекса инновационного развития и интеллектуальной собственности ОАО «Концерн «РТИ Системы».

С 2012 г. – заместитель генерального конструктора ОАО «РТИ». Первый заместитель председателя Научно-технического Совета ОАО «РТИ».

Кандидат технических наук (2001 г.), доцент (2012 г.). В 2002 г. награжден знаком «Почётный радист России».

Заместитель заведующего кафедрой «Интеллектуальные информационные радиофизические системы» МФТИ. Доцент МФТИ. Автор более 110 научных трудов.

О рецензенте и редакторе

БОЕВ Сергей Федотович.

Родился в 1953 году в г. Москве. В 1978 году окончил Всесоюзный юридический заочный институт. В 1984 году — Московский институт управления имени С.Орджоникидзе.

В 1971 — 1999 годах работал в Радиотехническом институте им. академика А. Л. Минца; прошел путь от ученика слесаря до генерального директора института.

В 2000 — 2008 годах — **генеральный директор** ОАО «Концерн «Радиотехнические и информационные системы». В 2008 — 2011 годах — **вице-президент**, руководитель бизнес-единицы «Высокие технологии и промышленность» ОАО АФК «Система». С 2011 года — **генеральный директор ОАО «РТИ»**. В 2012 году назначен **Генеральным конструктором национальной системы предупреждения о ракетном нападении (СПРН)**. В 2016 году избран **Предсе-**

дателем Совета директоров ОАО «РТИ» и назначен Генеральным конструктором ОАО «РТИ».

Доктор экономических наук, доктор технических наук, профессор, заслуженный экономист РФ.

Лауреат Государственной премии 2012 года в области науки и технологий.

Член Совета при Президенте РФ по модернизации экономики и инновационному развитию России и научного совета при Совете Безопасности РФ; сопредседатель рабочей группы по инновациям Круглого стола промышленников России и ЕС; действительный член Академии военных наук; заведующий кафедрой «Интеллектуальные информационные радиофизические системы» в МФТИ.

Является **Председателем Советов директоров**: ОАО «РТИ»; ОАО «Радиотехнический институт им. академика А. Л. Минца»; ОАО «Научно-производственный комплекс «Научно-исследовательский институт дальней радиосвязи».

Член Советов директоров: ПАО АФК «Система», АО «Концерн ВКО «Алмаз-Антей», АО «Технопарк «Саров».

Входит **в состав Попечительских советов**: Благотворительного фонда «Система», Клуба адмиралов России, Тверского суворовского военного училища, Некоммерческой организации «Фонд поддержки научной, научно-технической и инновационной деятельности ОАО «РТИ».