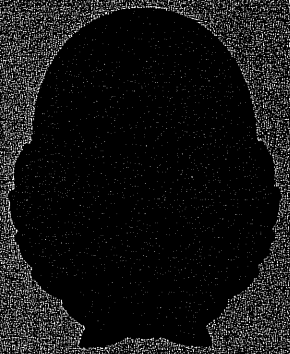
2-7 октября 2918 г.

Южный государственный технологический университет



СБОРНИК ДОКЛАДОВ XXII ПЛЕНУМА ФУМО ВО ИБ И ВСЕРОССИЙСКОЙ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ: КАДРЫ, ТЕХНОЛОГИИ, ПРАКТИКА»

Министерство науки и высшего образования Российской Федерации

Федеральное учебно-методическое объединение
в системе высшего образования
по УГСНП 10.00.00 «Информационная безопасность»

Кубанский государственный технологический университет

СБОРНИК ДОКЛАДОВ XXII ПЛЕНУМА ФУМО ВО ИБ И ВСЕРОССИЙСКОЙ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ: КАДРЫ, ТЕХНОЛОГИИ, ПРАКТИКА»

Краснодар
2018

УДК 004.45
ББК 32.972.5
С23

С23 **Сборник докладов XXII пленума ФУМО ВО ИБ и Всероссийской научно-практической конференции «Информационная безопасность регионов: кадры, технологии, практика»** / Отв. редактор: В.Н. Хализев; Федеральное учебно-методическое объединение в системе высшего образования по УГСНП 10.00.00 «Информационная безопасность»; Кубанский государственный технологический университет. – Краснодар : Издательский Дом – Юг, 2018. – 276 с.

Настоящий сборник содержит доклады XXII пленума ФУМО ВО ИБ и Всероссийской научно-практической конференции «Информационная безопасность регионов: кадры, технологии, практика».

Спонсоры конференции:

Автономная некоммерческая организация дополнительного профессионального образования **«Учебный центр «Информзащита»**;

Открытое акционерное общество **«Инфотекс»**;

Закрытое акционерное общество **«АТЭК-ХОЛДИНГ»**;

Коммерческий банк **«Кубань Кредит»** общество с ограниченной ответственностью;

Федеральное государственное унитарное предприятие **«Научно-производственное предприятие «Гамма»**;

Общество с ограниченной ответственностью **«Центр безопасности информации «МАСКОМ»**;

АО **«НПО РусБИТех»**.

ББК 32.972.5
УДК 004.45

СОДЕРЖАНИЕ

СЕКЦИЯ 1

«АКТУАЛЬНЫЕ ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ РЕАЛИЗАЦИИ ПРОГРАММЫ «ЦИФРОВАЯ ЭКОНОМИКА» (МЕТОДЫ, СРЕДСТВА И ТЕХНОЛОГИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ)

Буханов Д.Г., Поляков В.М.
Применение ИНС адаптивно-резонансной теории с многоуровневой памятью при решении задачи распознавания состояния компьютерной сети 8

Бурлаков М.Е., Осипов М.Н.
Применение метода Уорда для оптимизации атрибутного пространства набора данных информационных угроз CSIC 2010 HTTP DATASET 14

Гаршина В.В., Степанцов В.А.
Онтологический подход для анализа рисков безопасности информационных систем 20

Никитина Е.Ю.
Формирование личной информационной безопасности гражданина 24

Ткаченко Д.А., Сизоненко А.Б.
Программное обеспечение для хранения идентификационных данных, основанное на отечественных криптоалгоритмах 28

Тельный А.В., Монахов М.Ю., Романова А.Г., Яковлева Е.И.
О методике оценки защищенности организационного канала утечки информации на предприятии 33

Соляной В.Н., Сухотерин А.И.
Предпроектное моделирование организационных систем информационной безопасности 39

Бондакова О.С.
О первичной оценке вероятности возникновения коллизии для уменьшенного варианта хэш-функции «Стрибог» 43

Жмуров Д.Б., Сергеев В.В.
Новые угрозы информационной безопасности, обусловленные развитием технологий STT и IOT 48

Калита А.О., Ожиганова М.И.
Разработка системы блокирования акустических каналов утечки информации с адаптивным управлением 51

Кузнецова В.В., Безребрая И.С.
Лицензирование как инструмент регламентации отношений 59

Кузнецова В.В., Бузыкин К.С.
Исследования программного обеспечения российских разработчиков 63

Лебеденко А.В., Носенко А.А.
Концептуальные проблемы в реализации алгоритма разграничения доступа в децентрализованной корпоративной сети с использованием распределенных реестров и схемы разделения секрета 66

Максимова Е.А., Молодцова И.А., Бердник М.В.
Информационная гигиена как фактор предотвращения последствий z-цифровизации 70

Маслова М.А.
Принципы безопасности интернета вещей 76

Сидоркина И.Г., Кубашева Е.С., Соловьев М.Г., Галанина Н.А.
Подход к реализации алгоритмов работы с цифровым водяным знаком в аудиофайлах для систем защиты информации 82

Гончаренко Ю.Ю., Паво Ф.Н.
Разработка децентрализованного приложения для реализации цифровой идентичности с использованием технологии Блокчейн 88

Набока Ю.И.
Концептуальные основы противодействия системам технической разведки иностранных государств 94

Кулаков М.А., Цветов В.П.
Автоматизация подбора средств защиты информации в соответствии с законодательством в сфере защиты персональных данных 107

Карташевский В.Г., Крыжановский А.В.
Анализ методов и средств выявления инцидентов информационной безопасности 111

Московченко В.М., Шилина А.Н.
Совершенствование методики расчета показателей эффективности управления системой обеспечения безопасности автоматизированных систем управления в технологических процессах 116

Тищенко Е.Н., Палютина Г.Н.
Применение технологии оценки степени доверия заключений системы многофакторной аутентификации на основе алгоритма вероятностных экспертных систем 121

Шагапов И.А.
К вопросу о производстве качественной безопасной информации 125

Лимов М.Д., Гнутов Д.А., Осипов М.Н.
Некоторые аспекты применения методов когерентной оптики для регистрации виброакустического сигнала 128

Бондакова О.С.
О первичной оценке вероятности возникновения коллизии для уменьшенного варианта Хэш-функции «Стрибог» 134

Кулиш О.А., Королев И.Д.
Квантовые модели электрооптических фазовых модуляторов 138

Швырев Б.А.
Информационная безопасность. Актуальный аспект безопасности пенитенциарной системы 144

Минаев В.А., Королев И.Д., Сабанов А.Г.
Оценка рисков идентификации и аутентификации субъектов электронного взаимодействия 147

Минаев В.А., Петров С.С., Королев И.Д.
Проблемы и решения защиты информации внедоверенных средах: зарубежный опыт 155

Сафиуллина Л.Х., Касимова А.Р.
Анализ надежности хранения шаблонов при внедрении современных биометрических технологий в системы информационной безопасности 164

Власенко А.В., Корх И.А.
Дистанционное банковское обслуживание. Направления развития криптографической защиты в мобильных приложениях 169

Зязин В.П., Бердник М.В.
Оценка уровня стандартизации сквозной технологии «Больших данных» в Российской Федерации 174

Корх И.А., Чернецова Т.В., Позднякова Е.Г., Савинская Е.И.
Дистанционное банковское обслуживание. Направления развития криптографической защиты данных 180

Максимова Е.А., Баранов В.В., Зязин В.П.
Модель оценки рисков
при расследовании компьютерных преступлений 185

Хализев В.Н., Фёдоров С.Ю., Жданова Н.В.
Математическая модель синтеза интегрированной
системы безопасности на основе теории игр
и применения квалиметрической оценки качества 190

Угрюмов Д.В., Хализев В.Н.
Системная интеграция
программно-аппаратных компонент защиты 198

Частикова В.А., Жерлицын С.А., Воля Я.И.
Нейросетевой метод идентификации личности
по неформализованной семантической характеристике 210

Частикова В.А., Сотников В.В.
Метод анализа и идентификации
биометрических данных радужных оболочек глаз 218

Зангиев Т.Т., Частикова В.А.,
Тугушева З.Я., Гунай Ф.Р.
Анализ интернет-пространства
в условиях информационных противоборств 226

Частикова В.А., Зангиев Т.Т.,
Тугушева З.Я., Гунай Ф.Р.
Двухуровневая идентификация личности по логину/паролю и голосу 229

СЕКЦИЯ 2

ВОПРОСЫ ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (НАУЧНЫЕ, ПЕДАГОГИЧЕСКИЕ И МЕТОДИЧЕСКИЕ АСПЕКТЫ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ – ПРОБЛЕМЫ И РЕШЕНИЯ)

Афанасьевский Л.Б., Будников С.А.,
Горин А.Н., Фадин А.Г.
Методические рекомендации по подготовке
и проведению занятий по информатике в интерактивной форме 232

Пестряков А.В., Симонов П.И., Кубанков Ю.А.
Подход к формированию способности проводить
инструментальный мониторинг
качества защищённости телекоммуникационных систем 237

Степанов С.В.
Особенности подготовки специалистов (техников)
по специальности 10.02.05 «Обеспечение информационной
безопасности автоматизированных систем» в вузах
и образовательных организациях СПО 242

Сухотерин А.И., Соляной В.Н.
Становление организационно-профессиональных структур
по защите информации (обеспечению
информационной безопасности) в России 244

Крыжевич Л.С.
Разработка аппаратных средств
для закрытого WI-FI – тестирования студентов 250

Чефранова А.О., Кузьмин О.В.
Материально-техническое обеспечение дисциплин
по информационной безопасности при подготовке специалистов
в высших и средних учебных заведениях в сфере информационной
безопасности и технической защиты информации 256

Романчева Н.И.
Цифровая трансформация образования в области
информационной безопасности: риски и неопределенности 260

Корабельщикова С.Ю., Троицкая О.Н.,
Хаймина Л.Э., Хаймин Е.С., Ширикова Т.С.
О проекте «Основы кибербезопасности» 264

Цибуля А.Н., Беляков Э.В., Козачок А.И.
Формирование индикаторов достижения компетенций для группы
учебных дисциплин «Телекоммуникационные технологии»
специальности 10.05.02 «информационная безопасность
телекоммуникационных систем» на основе анализа требований
профессиональных стандартов 269

Для частных показателей, можно, например, установить следующую шкалу степени их выполнения: – «нет» – оценке присваивается значение, равное нулю; – «частично» – оценке присваивается значение 0,25, 0,5, или 0,75; – «да» – оценке присваивается значение, равное единице.

При проведении оценки частных показателей, для которых оценивается, как степень их установления в организации, так и степень выполнения можно использовать следующий общий подход: – оценка «0» если требования частного показателя не установлены во внутренних документах проверяемой организации; – оценка «0,25» если требования установлены во внутренних документах проверяемой организации, но не выполняются; – оценка «0,5» если требования установлены во внутренних документах проверяемой организации, но выполняются в неполном объеме; – оценка «0,5» если требования установлены во внутренних документах проверяемой организации и выполняются почти в полном объеме; – оценка «1» если требования частного показателя установлены во внутренних документах проверяемой организации и выполняются в полном объеме.

Полученные свидетельства оценки соответствия защищенности организационного канала утечки информации и источники их получения должны быть задокументированы путем составления листов для сбора свидетельств оценки соответствия защищенности организационного канала.

Если оценка K_i лежит в интервале от 0 до 0,25, то данному направлению оценки присваивается нулевой уровень соответствия требованиям нормативно-правовых документов по недопущению утечки информации по организационному каналу. Соответственно, от 0,25 до 0,5 – 1 уровень; от 0,5 до 0,7 – 2 уровень; от 0,7 до 0,85 – 3 уровень; от 0,85 до 0,95 – 4 уровень и от 0,95 до 9 – 5 уровень соответствия требованиям нормативно-правовых документов по недопущению утечки информации по организационному каналу. Для общей оценки защищенности организационного канала можно ввести интегральный показатель $R = \min\{K_1; K_2; \ldots K_{23}\}$, при этом используются только оцениваемые групповые показатели. Значения R соответствующие четвертому и пятому уровню, являются рекомендуемыми. При $R < 0,85$ защищенность организационного канала следует считать не удовлетворительной.

Полная методика, разработанная на кафедре информатики и защиты информации Владимирского государственного университета, использует более 500 частных показателей по 23 групповым показателям (табл. 2). Кроме того, по каждому частному показателю сформированы данные экспертных оценок v_{ij} важности и d_{ij} достоверности. При реализации методики, шкалы оценивания могут быть сформированы более подробно, чем предложеные авторами.

Литература

1. Тельный А.В. «Динамическая модель достаточности инженерно-технического укрепления элементов строительных конструкций территорий, зданий и помещений объектов для предотвращения несанкционированного доступа» Динамика сложных систем – XXI век / А.В. Тельный, М.Ю. Монахов. – 2016. – № 1. – С. 41–48. ISSN 1999-7493.

2. Тельный А.В. «Оценка защищенности информационных ресурсов организации от несанкционированного доступа нарушителей в здания и помещения» Известия высших учебных заведений. Технология текстильной промышленности / А.В. Тельный, Ю.М. Монахов, М.Ю. Монахов. – 2016. – № 5. – С. 259–263;

3. Тельный А.В. «Автоматизация оценки достаточности технических средств охраны и безопасности для защиты от несанкционированного доступа производственного объекта» Известия высших учебных заведений. Технология текстильной промышленности / А.В. Тельный, М.Ю. Монахов, Ю.М. Монахов. – 2016. – № 5. – С. 263–267.

УДК 621.31

ПРЕДПРОЕКТНОЕ МОДЕЛИРОВАНИЕ ОРГАНИЗАЦИОННЫХ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В.Н. Соляной, А.И. Сухотерин

Государственное бюджетное образовательное учреждение высшего образования Московской области «Технологический университет», 141070 Московская область, г. Королев, ул. Гагарина, д. 42, e-mail: solyanoy@ut-mo.ru

Состояние информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства характеризуется стремлением отдельных государств использовать технологическое превосходство для доминирования в информационном пространстве, и здесь без моделирования системы информационной безопасности объекта информатизации не обойтись. Фундаментальные характеристики организационной системы информационной безопасности являются ее структура (архитектура) и способ функционирования (поведение). При создании новых систем и реформировании или модернизации существующих необходимо, прежде всего, установить цели, поставленные перед системой, понять, достижимы ли они при реальных ограничениях на финансовые и временные ресурсы, и если достижимы, то какими должны быть измене-

Например, дисциплина «Физическая культура» формируется в соответствии с Наставлением по физической подготовке в ВС РФ.

В-пятых, ФГОС СПО по специальности 10.02.05 определяет проведение демонстрационного экзамена в ходе государственной итоговой аттестации, что трудно реализуемо в военных образовательных организациях с точки зрения сохранности сведений, составляющих государственную тайну.

Исходя из вышеизложенного, возникает необходимость в разработке отдельной ПООП для вузов МО РФ, которая изначально учитывает специфику подготовки военного специалиста (техника).

В образовательных организациях СПО в качестве заказчика подготовки выступают работодатели, для которых компетентностный поход в реализации образовательной программы является несомненным плюсом, т.к. у специалиста (техника) уже сформированы профессиональные компетенции, а не просто знания и умения, которые проверялись полнотой освоения учебных программ (профессиональных модулей) и не давало работодателям объективно оценить профессионализм выпускника.

Литература

1. Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

2. Примерная основная образовательная программа по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем (зарегистрирована в государственном реестре примерных основных образовательных программ под номером 10.02.05-170703).

УДК 004.56

СТАНОВЛЕНИЕ ОРГАНИЗАЦИОННО-ПРОФЕССИОНАЛЬНЫХ СТРУКТУР ПО ЗАЩИТЕ ИНФОРМАЦИИ (ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ) В РОССИИ

А.И. Сухотерин, В.Н. Соляной

Государственное бюджетное образовательное учреждение высшего образования Московской области «Технологический университет», 141070 Московская область, г. Королев, ул. Гагарина, д. 42, e-mail: solyanoy@ut-mo.ru

Исследование развития организационно-профессиональных структур по защите информации в историческом аспекте, в современных условиях и ходе формирования системы обеспечения информационной безопасности России, является весьма актуальной задачей [1, 2, 3, 4, 5].

В истории развития системы защиты информации на предприятиях России можно выделить три периода:

– первый – относится к тому времени, когда обработка информации осуществлялась по традиционным (ручным, бумажным) технологиям (в основном это период функционирования царской России);

– второй – когда для обработки информации на регулярной основе стали применяться технические средства обработки информации, в частности, телефон, телеграф и радиосредства (в основном это период существования Советского государства);

– третий – когда для обработки информации на регулярной основе стала применяться электронно-вычислительная техника, использование которой приняло массовый и повсеместный характер, появились персональные компьютеры и другая компьютерная мобильная техника (в основном это период возникновения и развития постсоветского государства – Российской Федерации).

Ключевые слова: Информационная безопасность, развитие системы защиты информации в России, организационно-профессиональные структуры.

Первый период (существования царской России) определяется началом создания осмыслен ных и самостоятельных средств и методов защиты информации и связан с появлением возможности фиксации информацион ных сообщений на твердых носителях, то есть с использованием письменности. При этом возникла проблема сохранения в тайне существующей уже отдельно от источника конфиденциальной информации, поэтому практически одно временно возникли такие методы защиты информации, как шифрование и скрытие.

С образованием Российского государства стали формироваться органы государственного управления и развиваться международные связи. Возникла необходимость защиты информации в области военной, внешне- и внутриполитической деятельности государства.

В период XV–XVII веков в России стали складываться элементы организации защиты информации, как предпосылки формирования организационной защиты информации.

С 1816 года отмечается начало использования искусственно создаваемых технических средств электро- и радиосвязи. Для обеспечения скрытности и помехозащищенности радиосвязи необходимо было использовать опыт первого периода информационной безопасности на более высоком технологическом уровне, а именно применение помехоустойчивого кодирования сообщения (сигнала) с последующим декодированием принятого сообщения (сигнала).

Отмечается регламентирование вопросов защиты информации в государственных учреждениях (Генеральный регламент 1720 г.) и др. меры.