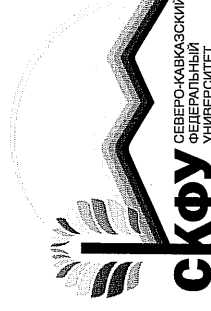
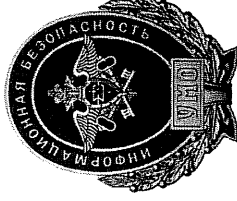


Министерство науки и высшего образования Российской Федерации
Федеральное учебно-методическое объединение в системе высшего
образования по УГСНП 10.00.00 Информационная безопасность
ФГАОУ ВО «Северо-Кавказский федеральный университет»



**СБОРНИК ДОКЛАДОВ
XXIII ПЛЕНУМА ФУМО ВО ИБ
И ВСЕРОССИЙСКОЙ НАУЧНОЙ КОНФЕРЕНЦИИ
«ФУНДАМЕНТАЛЬНЫЕ ПРОБЛЕМЫ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ»
(ИНФБЕЗОПАСНОСТЬ –2019)**

Ставрополь
2019

С23 **Сборник докладов XXIII пленума ФУМО ВО ИБ и Всероссийской научной конференции «Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации» (ИНФОБЕЗОПАСНОСТЬ –2019) / Отв. редактор: В.И. Петренко; Федеральное учебно-методическое объединение в системе высшего образования по УГСНП 10.00.00 Информационная безопасность ФГАОУ ВО «Северо-Кавказский федеральный университет»; ФГАОУ ВО «СевероКавказский федеральный университет». – Ставрополь: Изд-во СКФУ, 2019. – 300 с.**

Настоящий сборник содержит доклады XXIII пленума ФУМО ВО ИБ и Всероссийской научной конференции «Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации»

УДК 004.45
ББК 32.972.5

Спонсоры конференции:

ООО «Открытая мобильная платформа»
ООО «РусБИТех-Астра»
ООО «Монтажно-технологическое управление «Телеком-С»»
ООО «АЛЬФА»

© Коллектив разработчиков, 2019
© Федеральное учебно-методическое объединение в системе высшего образования по УГСНП 10.00.00 «Информационная безопасность», 2019
© ФГАОУ ВО «Северо-Кавказский федеральный университет», 2019

Содержание

СЕКЦИЯ 1. «ФУНДАМЕНТАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ»	7
Фрид А.И., Гузаиров М.Б., Вульфрин А.М., Берхольц В.В. Концепция мониторинга целостности телеметрической информации о состоянии энергетической установки летательного аппарата.....	7
Таньгин М.О., Алшана Х.Я., Хемраев Д. Использование метаданных для исправления ошибок аутентификации при сетевом взаимодействии.....	14
Поляков В.М., Буханов Д.Г., Релькина М.А., Кальтов И.В. Применение искусственных нейронных сетей адаптивно-резонансной теории при классификации PE-файлов.....	18
Лебеденко А.В., Гончаренко Ю.Ю., Нестеренко В.Р. Система биометрической идентификации пользователя на основе сверточной нейронной сети для небольшой организации.....	22
Ивкин А.Н., Бураков М.Е. Использование алгоритмов машинного обучения в сетевой системе обнаружения и предотвращения вторжений.....	25
Баранов В.В., Алиев Э.Р., Игнатьева А.Р. Исследование алгоритмов целенаправленных компьютерных атак на элементы инфокоммуникационных сетей.....	30
Лимов М.Д., Домашева А.С., Осипов М.Н. Лазерная интерференционная система периметровой охраны объектов информатизации.....	36
Иевлев О.П., Шелухин О.И., Большаков А.С., Раковский Д.И. Моделирование угроз информационной безопасности с использованием банка данных ФСТЭК.....	41
Чекулаева Е.Н., Гушина Е.В. Источники и виды угроз информации в информационной и экономической безопасности.....	47
Радионов А.В. Определение охраняемых сведений об образце военной техники.....	51
Соляной В.Н., Сухотерин А.И. Совершенствование организационной деятельности службы информационной безопасности на основе процессного подхода.....	55
Ильченко А.Н. Математическая модель и методика оценки угроз безопасности информации в информационной системе в условиях неопределенности.....	60
Корепанов А.Г., Трубин И.С. Информационно-поисковая система для выбора технических средств защиты информации.....	65
Галанина Н.А., Иванов П.Б., Кубашева Е.С. К вопросу об эффективности использования системы остаточных классов для криптографической защиты информации.....	70
Грובה Т.А., Кулибачук М.Г. Защита данных в беспроводных сетях.....	75
Заводнов В.С. Проблемы безопасности в беспроводных сетях стандарта IEEE 802.11.....	79
Власенко А.В., Корх И.А. Проблемы информационной безопасности базовой автоматизированной банковской системы.....	82
Лужнов В.С., Соколов А.Н. Использование эталонных моделей безопасности автоматизированных систем управления технологическими процессами на основе связанных ациклических графов в процессах моделирования защищенных систем.....	88

Карлова Н.Е., Панфилова И.Е. К вопросу обеспечения безопасности информационных процессов в социотехнических системах	95	СЕКЦИЯ 2. «ВОПРОСЫ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»	201
Басан Е.С., Веселов Г.Е. Моделирование элементов системы группового управления мобильными роботами с целью анализа их защищенности	100	Цельх А.Н., Котов Э.М. Об опыте организации обучения дисциплине «Компьютерные расследования» специалистов по информационной безопасности	201
Басан Е.С., Веселов Г.Е., Басан А.С., Абрамов Е.С. Исследование методов и средств защиты для группы мобильных роботов с учетом требований российского и зарубежного законодательства	107	Чемарина Ю.В., Шаповалова И.А. Об особенностях подготовки специалистов по информационной безопасности на математическом факультете Тверского государственного университета	205
Некрасова Е.А., Чайка Е.А., Грובה Т.А. Анализ достоинств и недостатков основных методов обеспечения контроля целостности файлов	115	Афанасьевский Л.Б., Будников С.А., Жуматий В.П., Фадин А.Г. Методические особенности проведения военно-специальной игры при подготовке специалистов по информационной безопасности	212
Румянцев К.Е., Шакир Х.Х. Перспективы применения квантового распределения ключа по протоколу B92	121	Романчева Н.И. О формах оценки степени подготовленности специалистов в области информационной безопасности	220
Крыженич Л.С., Бабкин Г.В. Имитационная модель безопасного цифрового взаимодействия "Кибергород 2.0"	128	Цветов В.П. Расследование компьютерных инцидентов и преступлений (структура образовательных программ)	226
Тельный А.В., Монахов М.Ю., Монахов Ю.М. Об оценке параметров, подлежащих защите информационных ресурсов организации, по имеющимся эмпирическим данным их аналогов	132	Чернова И.В. Особенности высшего образования в области информационной безопасности	234
Чекулаева Е.Н., Гушина Е.В. Средства защиты информационной безопасности автоматизированной системы «Отдел кадров»	138	Пестряков А.В., Симонов П.И., Корухин И.С. Формирование стандартных компетенций по организации радиоэлектронного производства с учётом информационной безопасности	237
Гончаров Н.И., Гаршина В.В., Сирота А.А. Модели конфликтного взаимодействия систем на основе формализма гибридных автоматов и их применение в задачах анализа безопасности облачных технологий	142	Маро Е.А., Ипучкова Е.А., Веселов Г.Е. Повышение профессиональных компетенций специалистов по защите информации на основе реализации игровых сценариев обучения	242
Сычев А.Д., Гоголя В.А., Минкина Т.В., Бушуров А.Д. Разработка защищенных протоколов интернета вещей для распределённых энергетических сетей	149	Никитина Е.Ю. Разработка программы личной информационной безопасности гражданина Пермского края	247
Максимова Е.А. Исследование алгоритмов безопасной передачи данных между объектами критической информационной инфраструктуры	157	Жукова М.Н. Золотарев В.В. Опыт магистерской подготовки в области ИБ в Красноярском крае	250
Забокрицкий Е.И., Грובה Т.А. Инженерно-технические средства защиты информации	163	Цибуля А.Н., Козачок А.И. Особенности подготовки специалистов в области защищенных операционных систем с учетом требований образовательных и профессиональных стандартов	253
Османов А.А., Грובה Т.А. Основные методы биометрического контроля и аутентификации, используемые в банковской системе Российской Федерации	166	Ветров И.А., Перичкин А.А. Практическое реализация инновационных методов обучения для повышения качества переподготовки специалистов по информационной безопасности в региональных учебно-научных центрах	259
Воробьев Г.А., Павленко И.И., Рындюк В.А., Писаренко Е.А. Использование вероятностных моделей крипто преобразований при дистанционном заключении многосторонних договоров в онлайн режиме	169	Иванцов А.М., Сергеев В.В., Ратеев С.М., Жмуров Д.Б. Проектирование индикаторов достижения компетенций примерной ООП по ФГОС (3++) для специализации "безопасность открытых информационных систем" специальности 10.05.03	264
Сапрыкина А.А., Суховицкая В.Е. Анализ атак на беспроводные сети Интернета вещей и способы её защиты	176	Дурнев В.Г., Зеткина О.В. Об одном подходе к выполнению "Примерного учебного плана подготовки специалиста по специальности «Компьютерная безопасность»"	268
Соловьева И.В., Мандрица И.В., Петренко В.И., Колыгтов В.В., Жук А.П., Мандрица О.В., Рачков В.Е., Антонов В.В., Минкина Т.В. Методика технико-экономического обоснования проектных решений по информационной безопасности	183		
Соляной В.Н., Сухотерин А.И. Технологические основы построения интеллектуальных систем прогнозирования инцидентов информационной безопасности	194		

Шиверов П.К., Варюхина А.Д., Дружинин М.В., Осипов М.Н. Организация самостоятельно развивающегося сообщества молодых специалистов в области информационной безопасности.....	273
Абрамов Е.С., Басан Е.С., Пескова О.Ю. Внедрение материалов и технологий Worldskills в учебный процесс при подготовке специалистов по информационной безопасности.....	276
Сизов В.А. Применение деловых игр в освоении компетенций магистрами по направлению подготовки «Информационная безопасность».....	291
Лобанов М.И., Горбатов В.С., Васильев А.А. К вопросу о подготовке кадров по безопасности объектов КИИ.....	296

СЕКЦИЯ 1. «ФУНДАМЕНТАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ»

Концепция мониторинга целостности телеметрической информации о состоянии энергетической установки летательного аппарата

А.И. Фрид
Уфимский государственный авиационный
технический университет
Уфа, Россия
e-mail: frid46@mail.ru

М.Б. Гузаиров
Уфимский государственный авиационный
технический университет
Уфа, Россия
e-mail: guzaikov@ugatu.su

А.М. Вульфин
Уфимский государственный авиационный
технический университет
Уфа, Россия
e-mail: vulfin.alexey@gmail.com

В.В. Берхольц
Уфимский государственный авиационный
технический университет
Уфа, Россия
e-mail: tofina4@yandex.ru

Аннотация

Рассмотрены вопросы создания системы мониторинга целостности накапливаемых данных в модульной системе сбора, хранения и обработки телеметрической информации о состоянии энергетической установки летательного аппарата на основе применения ее модели и современных технологий интеллектуального анализа телеметрической информации.

Ключевые слова: система сбора, хранения и обработки телеметрической информации, автоматизированная информационная система, целостность данных измерений, модель энергетической установки.

1. Введение

В настоящее время эксплуатируется и разрабатывается множество типов энергетических установок (ЭУ) летательного аппарата (ЛА): газотурбинные, электрические, на ядерном топливе, ракетные двигатели и т.д. Повышение эффективности обслуживания ЭУ ЛА

возможно, в частности, за счет снижения времени, затрачиваемого на контроль и диагностику его технического состояния, что требует использования оперативных и эффективных методов контроля на основе комплексной автоматизации и интеллектуализации. Эффективность контроля состояния ЭУ существенно зависит от вероятности корректного определения его технического состояния, что определяет экономичность и безопасность полетов [1, 2].

Развитие технологий контроля параметров ЭУ связано с совершенствованием алгоритмического и математического обеспечения информационных систем, позволяющего учитывать нестационарность физических процессов при эксплуатации, сложность их математического описания, зависимость технических характеристик от внешних условий работы, ограниченный состав измеряемых параметров, их технологический разброс и т.д. [1, 2].

Цифровые системы управления ЭУ содержат встроенные системы контроля и диагностики

«1», с множеством элементов облика S_j , изначально не подлежащих защите (при этом, если мера включения на 5-м шаге получилась равной меньше «1», то делается вывод, что элемент облика S_j не подлежит защите):

$$C_{\text{эк}}(S_j^{\text{зам}}, S_j) = \frac{2 \text{card}(S_j^{\text{зам}} \cap S_j)}{\text{card}(S_j^{\text{зам}}) + \text{card}(S_j)}, \quad (6)$$

$$V_{S_j^{\text{зам}}} | M_{\text{эк}}(S_j^{\text{зам}}, B) = 1.$$

На седьмом шаге по максимуму значения меры сходства определяются элементы облика ОВТ изначально не отнесенные к защищаемым, которые подлежат защите:

$$S_j^* = S_j | C_{\text{эк}}(S_j^{\text{зам}}, S_j) = \max_{S_j \in S} C_{\text{эк}}(S_j^{\text{зам}}, S_j). \quad (7)$$

На восьмом шаге полученные элементы облика S_j^* исключаются из матрицы совокупного объема сведений B и осуществляется выполнение шага 5 (определение меры включения $M_{\text{эк}}$ элементов облика $S_j^{\text{зам}}$ в полученное множество матрицы B совокупного объема свойств элементов облика ОВТ, не подлежащих защите). При этом значение пятого шага $M_{\text{эк}}(S_j^{\text{зам}}, B) < 1$ возвращает последовательность действий и формируются полученные искомые элементы облика S_j^* , подлежащие защите.

4. Результаты

Результатом работы является методика, основанная на методе морфологического анализа и позволяющая с учетом семантических связей облика ОВТ решить актуальную задачу по определению его ОС.

На основе предложенной методики разработана «Программа определения защищаемых элементов изделия» [7].

5. Заключение

В данной статье представлена методика определения охраняемых сведений об объеме военной техники, основывающаяся на

методе морфологического анализа и учитывающая семантические связи между элементами облика ОВТ. Применение данной методики для определения охраняемых сведений об образце военной техники позволяет снизить субъективность экспертных оценок.

Список используемых источников

1. Федеральный закон Российской Федерации от 1 июля 1993 года № 5485-1 "О государственной тайне" // Собрание законодательства РФ. – 1993. – № 41. – С. 8220-8225.
2. Модель облика образца вооружения и военной техники на этапах жизненного цикла изделия / А.В. Радиков, В.А. Мельник // Научно-практический межрегиональный журнал «Стратегическая стабильность», выпуск №4 (85), 2018г.: 61 – 63.
3. Исследовательский Центр Виктора Воксаня [Электронный ресурс]. Информационный бюллетень № 33 (октябрь 2013 г.). – URL: <http://viktorokskanayev.narod.ru/vokskanayev.html> (дата обращения: 08.09.2019)
4. Анализ информационных процессов на этапе жизненного цикла образцов вооружения и военной техники / А.В. Радиков // Труды 41ПФ Минобороны России. Материалы Всероссийской научно-технической конференции «Создание и развитие средств защиты информации и информационного противоборства в РВСН» – 2018. Вып. №142, т.1, ч.1 – С.134-136.
5. Формирование облика образца вооружения и военной техники на этапах научно-исследовательских и опытно-конструкторских работ / А.В. Радиков // Сборник научных трудов «Проблемы обороноспособности и безопасности», вып. №19, ФГВНУ «Аналитический центр», 2018г. С.76-79.
6. Андрейчикова А.В., Андрейчикова О.Н. Анализ, синтез, планирование решений в экономике. Учебник – 2-е изд., дополненное и переработанное – М.: Финансы и статистика, 2004. 464 с.
7. Свид. 2019660121 Российская Федерация. Способ определения об официальной регистрации программ для ЭВМ. Программа определения защищаемых элементов изделия / А.В. Радиков, В.А. Мельник, В.А. Мельник; заявитель и правообладатель А.В. Радиков (RU). – №201961911, заявл. 17.07.2019; опубл. 30.07.2019. Регистр программ для ЭВМ. – 1 с.

Современствование организационной деятельности службы инфорационной безопасности на основе процессного подхода

В.Н. Соляной

Институт техники и цифровых технологий
Технологический университет
Г. Королев, МО, Россия
e-mail: solyanov@it-mo.ru

Аннотация

Переход к процессному управлению требует от компаний функционального описания сфер деятельности их подразделений, но далеко не все на практике справляются с этой задачей. Однако, существуют определенные методы составления формализованного описания. Один из важных моментов – применение текущего, организационного и правового анализа для организации деятельности Службы ИБ [1, 2, 3, 4, 5, 6, 7].

Анализируя в различных организациях положения о подразделении ИБ, нередко отсутствуют в них ключевые разделы, например, раздела «Подпомощью», а также с абстрактными формулировками функций и задач. Казалось бы, руководителю нет ничего проще, чем сформулировать в положении об отделе, какую работу он фактически выполняет (см. левый столбец табл. 1).

Как видно из табл. 1, в результате формирования все получается не так однозначно, как хотелось бы. Непрудуно увидеть различия между данными в левом и правом столбце, но вот как перейти от первого варианта ко второму? За какую простотой темы скрывается весьма сложная методическая работа, которой часто не уделяется должного внимания.

Ключевые слова: информационная безопасность; прогнозирование; под-

А.И. Сухотерин

Институт техники и цифровых технологий
Технологический университет
Г. Королев, МО, Россия
e-mail: sukhoterina@it-mo.ru

Разделение информационной безопасности, компетентности, процессный подход.

1. Введение

Для начала необходимо определить используемую систему ценностей – именно логически взаимосвязанную систему (например, такую, как на рисунке), а не фрагменты знаний из различных систем.

Пример, что в приведенной модели сфера деятельности расширяется как работа, выполнение которой базируется на компетентности сотрудников и компетенциях подразделения (иногда вместо «сферы деятельности» употребляют термин «зона ответственности»). Навязать здесь в явной форме не узаконены, поскольку они являются производными от умений [1, 4, 5, 6, 7].

Объекты – то, чем/кем управляет или что/кого контролирует подразделение. Объекты делятся на программное обеспечение, аппаратное, организационное и кадровое.

2. Функции и задачи подразделения

Функция – деятельность объекта в рамках некоторой системы и конкретные действия, совершаемые над управляемым или контролируемым объектом. В технике и в психологии, выражаясь обычным языком, функция обозначает принадлежность к чему-либо, что применяется для ускорения, решения задачи, намерений, достижения цели. Функция может являться частью процесса. В рамках подразделения функция бывает основными и дополнительными.

Технологические основы построения интеллектуальных систем прогнозирования инцидентов информационной безопасности

В.Н. Соляной

Институт техники и цифровых технологий

Технологический университет

г. Королёв, МО, Россия

e-mail: solyanou@ut-mo.ru

А.И. Сухотерин

Институт техники и цифровых технологий

Технологический университет

г. Королёв, МО, Россия

e-mail: slkhotein@ut-mo.ru

АННОТАЦИЯ

Построение систем прогнозирования инцидентов информационной безопасности (ИБ) в настоящее время рассматривается как одна из сложных и важных задач стоящих перед руководством защищаемых информационных объектов в современных условиях ведения скрытой информационной войне как на межконтинентальных и континентальных пространствах, так и в региональных и локальных сферах применения различных информационных систем. Системы прогнозирования, которые позволяют осуществлять сбор информации и по ключевым признакам ее анализировать с целью выявления инцидентов информационной безопасности в соответствии с заданным методом их обнаружения и реализуемой стратегией информационной безопасности, а также осуществлять ответные действия. Наличие разноаспектных защищаемых информационных систем требует выработки разных подходов по выбору технологических основ построения наиболее целесообразных систем прогнозирования инцидентов информационной безопасности. Целью данной статьи является обобщение технологических основ построения, прежде всего интеллектуальных систем прогнозирования инцидентов информационной безопасности как наиболее эффективных в состоянии усилившихся скрытых угроз для критически важных информационных инфраструктур. В статье пред-

ложен интеллектуальный подход построения систем прогнозирования инцидентов информационной безопасности в интересах реализации на защищаемых информационных объектах уже апробированной стратегии обеспечения ИБ [Малков]. Использование методов интеллектуальной аналитики позволяет снизить вычислительную сложность построения систем прогнозирования инцидентов, вошедших в известную момент времени и оперативно выработать ответные действия.

Ключевые слова: информационная безопасность; прогнозирование; интеллектуальные подходы; инциденты; информационная система; критическая инфраструктура; методы; модель.

1. Введение

Интеллектуальные системы прогнозирования инцидентов информационной безопасности представляют собой совокупность баз знаний и баз данных о произошедших инцидентах информационной безопасности, математических и логических методов сбора и обработки, анализа исходных данных в интересах прогнозирования инцидентов с целью выработки и принятия управленческих решений по информационной безопасности. Поиск и своевременное выявление инцидентов информационной безопасности на основе предшествующих или возникающих различных аномальных активности рассматривается как одна из ключевых проблем в области информационной бе-

зопасности предприятий (организаций и учреждений). Такой поиск и выявление инцидентов в современных условиях реализуется различными подходами (методами). Используя новейшие информационные технологии обработки больших данных (Big Data) с различными методами обнаружения, распознавания и прогнозирования различных информационных ситуаций позволяют разрешать упомянутую выше проблему в области обеспечения информационной безопасности. Методы Big Data позволяют для анализа информационной обстановки задействовать и осуществлять сверху (на основе статистики) большого количества источников и прогнозировать возможные инциденты информационной безопасности с реализацией следующих технологий:

- обнаружения скрытых тенденций в больших наборах данных на основе их анализа;
- непосредственного прогнозирования различных ситуаций;
- вычислять вероятность любого возможного инцидента (исхода);
- оперативно получать желаемые результаты прогноза и др.

Наша цель - рассмотреть в условиях фактора защищаемых информационных систем для различных предприятий (организаций и учреждений) обуславливая при этом различные алгоритмы построения защищаемых информационных систем прогнозирования инцидентов информационной безопасности. Литература по данной теме представляет многочисленные разработки и обуславливает актуальность исследований в современном мире. В последнее время в сфере исследований были рассмотрены большое количество различных подходов для построения адаптивных информационных систем прогнозирования инцидентов информационной безопасности на основе прогнозирования изменений параметров временных рядов [4] сигнатурный метод поиска по ключевым признакам [5], нейронные сети автоматического распознавания признаков [4], и др. Адаптивная информацион-

ная система прогнозирования при функционировании в нечетерминированной среде позволяет подстраиваться под изменение условий и ограничения окружающей анализируемой информационной среды.

Анализ существующих решений отражает индивидуальность использования разработанных подходов под конкретную информационную ситуацию и используемые методы, выявление и обоснование основ построения информационных систем прогнозирования инцидентов информационной безопасности с использованием различных условий и факторов функционирования защищаемых предприятий (организаций и учреждений) является актуальной задачей.

2. Постановка задачи

Целью данной статьи следует рассмотреть описание технологических основ построения интеллектуальных информационных систем прогнозирования инцидентов информационной безопасности для различных по масштабу деятельности предприятий (организаций и учреждений). Основной задачей работы является технологическое обоснование наиболее целесообразного подхода реализации с использованием метода интеллектуального анализа данных - нейросетевого прогнозирования.

Задачу исследования в данной постановке можно разделить на три уровня:

- стратегический уровень прогнозирования инцидентов. На данном уровне решается вопрос глобального прогнозирования (в интересах долгосрочного планирования информационной безопасности). Данная задача наиболее полно отражает потребности обеспечения информационной безопасности крупных распределенных предприятий (организаций и учреждений);
- тактический уровень прогнозирования инцидентов (в ходе краткосрочного планирования информационной безопасности). Данная задача прогнозирование тактического уровня сводится к решению задачи обеспечения информационной безопасности малых