Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056.5:681.586

Богдан Дмитрий Сергеевич

Модели угроз кибербезопасности систем “умный дом” для различных архитектур

АВТОРЕФЕРАТ

диссертации на соискание степени магистра технических наук
по специальности 1-39 81 03 Информационные радиотехнологии

_____
(подпись магистранта)

Научный руководитель

Половеня Сергей Иванович
(фамилия, имя, отчество)

Кандидат технических наук, доцент
(ученая степень, ученое звание)

_____
(подпись научного руководителя)

Минск 2020

КРАТКОЕ ВВЕДЕНИЕ

В настоящее время организация режима информационной безопасности (ИБ) становится критически важным стратегическим фактором для любой автоматизированной системы. Актуальность и необходимость применения процедур оценки и управления угрозами и рисками ИБ неуклонно возрастает в связи с повышением роли систем «Умный дом» и технологий в современном мире.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Представленная работа написана на тему «Модели угроз кибербезопасности систем “умный дом” для различных архитектур».

Объектом исследования является централизованная автоматизированная электронная система контроля, анализа состояний и управления локальными физическими объектами (управляющие механизмы, устройства и системы) в решении «Умный дом».

Цель исследования: выявление уязвимостей в решениях «Умный дом» с последующей разработкой модели угроз кибербезопасности, реализация которых приводит к несанкционированному доступу к личным данным пользователя, а также нарушению штатного функционирования решения.

Для достижения поставленной цели были сформулированы следующие **задачи:**

1. Изучить и проанализировать существующие алгоритмы и методики оценки угроз и рисков ИБ систем “Умный дом”, сделать выводы об их достаточности и применимости в производственной деятельности;
2. Разработать алгоритм и методику моделирования рассуждений эксперта при оценке угроз ИБ;
3. Разработать алгоритм и методику оценки вероятностей угроз ИБ систем “Умный дом”, минимизирующую участие экспертов в области ИБ;
4. Разработать алгоритм и методику прогнозирования угроз ИБ УД на краткосрочный период для предприятий государственного и негосударственного сектора;
5. Разработать программное обеспечение (ПО), на основе сконструированных алгоритмов и методик, и провести опытную эксплуатацию его работоспособности на базе организаций Республики Беларусь.

Личный вклад соискателя: предложены алгоритм и метод для оценки качества информационной безопасности. Произведена оценка информационного обеспечения для анализа качества защиты информации систем “Умный дом”.

Объект исследования: киберфизические, автоматизацизированные системы типа «Умный дом».

Предмет исследования: угрозы безопасности систем «Умный дом».

Степень изученности проблемы: Рассмотренная нормативно-правовая база (технические нормативно-правовые акты и стандарты) в области обеспечения информационной безопасности является основой построения системы защиты киберфизических систем (в том числе «Умный дом»). В то же время скорость развития информационных технологий значительно превышает скорость создания новых и сопровождения существующих нормативно-правовых актов в данной сфере. В соответствии с этим должны разрабатываться и применяться внутренние локальные нормативные правовые акты, регламентирующие вопросы управления информационной безопасностью киберфизических систем (стандарты организаций, регламенты, инструкции, положения и др.).

Многочисленность элементов, составляющих киберпространство, обилие взаимосвязей между ними, возможность применения специальных техник управления действиями этих элементов определяют развитие угроз кибербезопасности. Необыкновенно высокая и все нарастающая интенсивность атак происходит от громадных масштабов киберпространства, всевозможных и разнохарактерных связей между ними. Сложные атаки, имеющие комплексную структуру, опираются на возможность различных направлений распространения информации и сигналов. Использование методов социальной инженерии позволяет изыскивать наиболее продуктивные методы организации атак. В киберпространстве могут развиваться все более опасные и сложные угрозы. Они используют особенности его построения для достижения максимального эффекта. Кибербезопасность имеет целью решение этих вопросов и обеспечение нормального функционирования киберпространства, защищая его от возникающих угроз эффективным образом.

Кибербезопасность – совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями.

Кибербезопасность не может быть направлена на защиту от максимального числа угроз. Нужно обеспечить максимально благоприятную среду для работы пользователей и всех систем в киберпространстве.

При обеспечении кибербезопасности важно учитывать особенности киберпространства и ее наиболее важный аспект – наличие взаимосвязей между участниками (пользователями), что приводит к возможности возникновения синергетического эффекта.

Под **угрозой кибербезопасности** понимается потенциально возможное случайное или преднамеренное событие, процесс или явление, приводящее к нарушению кибербезопасности или поддерживающей ее инфраструктуры, которое наносит ущерб владельцу или пользователю системы киберпространства.

Нарушитель – это лицо, умышленно или неумышленно предпринявшее попытку реализации угрозы кибербезопасности, независимо от предпосылок и используемых методов и средств.

Под **атакой** понимается любое действие нарушителя, которое приводит к реализации угрозы путем использования уязвимостей программного и/или аппаратного обеспечения системы «Умный дом» (далее – система).

Под **уязвимостью системы «Умный дом»** понимается любая характеристика или свойство сетевого или системного компонента системы, использование которого нарушителем может привести к реализации угрозы.

Классификация нарушителей осуществляется по следующим критериям: сфера воздействия нарушителя на систему, способ, полномочия доступа к системе, мотивы нарушений, техническая квалификация нарушителя. Классификация угроз осуществляется по следующим критериям: источник угрозы, цель, объект и метод воздействия угрозы.

Цель исследования: Целью работы является решение научно-технической задачи разработки новых моделей и алгоритмов для качественной оценки ИБ, направленных на повышение эффективности обеспечения информационной безопасности в системах с технологией “Умный дом”.

Задачи исследования:

- Изучить и проанализировать существующие алгоритмы и методики оценки угроз и рисков ИБ систем “Умный дом”, сделать выводы об их достаточности и применимости в производственной деятельности;
- Разработать алгоритм и методику моделирования рассуждений эксперта при оценке угроз ИБ;
- Разработать алгоритм и методику оценки вероятностей угроз ИБ систем “Умный дом”, минимизирующую участие экспертов в области ИБ;
- Разработать алгоритм и методику прогнозирования угроз ИБ УД на краткосрочный период для предприятий государственного и негосударственного сектора;
- Разработать программное обеспечение (ПО), на основе сконструированных алгоритмов и методик, и провести опытную эксплуатацию его работоспособности на базе организаций.

Методологической основой работы является комплексный подход. Для решения поставленных задач применялись следующие методы:

- анализ стандартов и архитектур информационной безопасности киберфизических систем
- программный анализ
- создание программного обеспечения.

Научная новизна: впервые было разработано программное обеспечение, для оценки угроз и рисков информационной безопасности систем «Умный дом».

Практическая и научная значимость: основные положения проведенного исследования могут лечь в основу дальнейших теоретических и практических разработок. Результаты диссертации могут быть использованы при анализе систем типа «Умный дом» в жилых помещениях, а также офисных и производственных помещениях на предприятиях малого и среднего бизнеса.

Границы исследования: основной акцент ставился на изучении существующих методик оценки угроз и рисков информационной безопасности автоматизированных систем и создании ПО на основе собственной методики.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность исследования, ставятся цели и задачи, определяются предмет, объект исследования, научная новизна и практическая ценность.

В первой главе был проведен анализ международных и зарубежных стандартов обеспечения информационной безопасности в области информационных технологий.

Информация, полученная при анализе существующих стандартов использовалась при дальнейшем изучении существующих архитектур системы «умный дом». В работе были рассмотрены следующие виды архитектур системы «Умный дом»:

- централизованная архитектура системы «Умный дом»,
- автономная централизованная архитектура,
- зависимая централизованная архитектура,
- децентрализованная архитектура,
- гибридная архитектура.

Полученная информация была применена при разработке модели угроз кибербезопасности.

Во второй главе проанализированы международные и существующие в Республике Беларусь стандарты безопасности в системах автоматизации помещений, их особенности. Рассмотренная нормативно-правовая база может служить основой при разработке и формировании подхода к определению вероятности угроз утечки информации, их прогнозированию и предотвращению. Предложенные алгоритмы и методики позволяют исключить ошибки экспертов при определении угроз информационной безопасности, учесть их в явном виде, сократить степень участия экспертов в данном процессе и временные затраты на него.

К международным стандартам были отнесены и рассмотрены следующие стандарты:

- EN 15232 Влияние автоматизации на энергоэффективность зданий;

– ENISO 16484-1 Обзор. Термины и определения;

– EN ISO 16484-2 Аппаратные средства;

– ENISO 16484-3 Стандартизация функций систем анализа защищенности (САЗ);

– ENISO 16484-4 Приложения комнатной автоматизации;

– ENISO 16484-5 Открытые протоколы связи для САЗ;

– ENISO 16484-6 Проверка соответствия;

– ENISO 16484-7 Технические требования к интегрированным системам.

Специальные стандарты для основных инженерных систем:

– EN 15316-1 и EN 15316-4 Отопление;

– EN 15243 Охлаждение;

– EN 15316-3 Горячее водоснабжение;

– EN 15241 Вентиляция;

– EN 15193 Освещение.

Среди стандартов Республики Беларусь одним из важнейших документов в области в области информационной безопасности является «Постановление Совета Безопасности Республики Беларусь о концепции информационной безопасности Республики Беларусь» от 18.03.2019 года. Кроме того, были изучены «Концепция национальной безопасности Республики Беларусь», законы Республики Беларусь «Об информации, информатизации и защите информации», «О государственных секретах», «Об электронном документе», «Об оценке соответствия требованиям технических нормативных актов в области технического нормирования и стандартизации», «О техническом нормировании и стандартизации» и другие.

Далее были даны классификации угроз кибербезопасности по следующим критериям:

1. Классификация субъектов, реализующих угрозы кибербезопасности. По сфере воздействия на систему, потенциальных нарушителей можно разделить на внутренних и внешних.

   Под **внутренними нарушителями** подразумеваются лица, имеющие физический и/или логический доступ к ресурсам системы (программно техническим и/или информационным).

   Под **внешними нарушителями** подразумеваются физические лица, имеющие физический и/или логический доступ к ресурсам системы (программно-техническим и/или информационным), получившие доступ незаконным способом.

2. Классификация источников угроз кибербезопасности.

   По сфере воздействия на систему «Умный дом» источники угроз можно разделить на внутренние и внешние.

   По мотивации воздействия на ресурсы системы, источники угроз кибербезопасности можно разделить на преднамеренные и случайные.

Преднамеренные (умышленные) угрозы связаны с корыстными стремлениями людей (злоумышленников).

Случайные (неумышленные) угрозы вызваны ошибками в проектировании элементов системы, в программном обеспечении, в действиях пользователей и т. п.

В третьей главе приведено описание ПО для разработанного подхода определения угроз ИБ КФС «Умный дом», основывающееся на поэтапном использовании алгоритмов и методик. Проведено описание алгоритмов функционирования ПО, его основных классов и обязательных файлов, среды разработки ПО и руководства по его использованию.

На тестовых примерах из практической деятельности различных организаций осуществлена проверка работоспособности ПО.

Детальный код ПО представлен в Приложении В.

ЗАКЛЮЧЕНИЕ

В процессе выполнения магистерской работы был выполнен анализ уязвимости технических средств, существующих угроз ИБ, а также существующих алгоритмов, методик оценки угроз и уязвимостей ИБ. Были предложены алгоритм и методика оценки ущерба от реализации угроз ИБ КФС «Умный дом», позволяющие классифицировать виды ущерба и определять его количественные показатели в результате реализации угроз ИБ.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1. Богдан Д. С. / Методическое обеспечение оценки угроз и рисков информационной безопасности систем “умный дом”. XX научно-техническая конференция аспирантов, студентов и молодых специалистов Белорусской государственной академии связи «Новые информационные технологии в телекоммуникациях и почтовой связи», », 12-13 мая 2020 года.

2. Богдан Д. С. / Методическое обеспечение оценки угроз и рисков информационной безопасности систем “умный дом”. 56-я научная конференция аспирантов, магистрантов и студентов БГУИР, », 18-20 мая 2020 года.