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

УДК 004.056.53:373

НЕСТЕРОВИЧ
Юрий Николаевич

МОДЕЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УЧРЕЖДЕНИЙ ОБЩЕГО СРЕДНЕГО ОБРАЗОВАНИЯ

АВТОРЕФЕРАТ
на соискание степени магистра

по специальности 1-98 80 01 «Информационная безопасность»

Научный руководитель

Листопад Николай Измаилович
доктор техн. наук, профессор,
зав. кафедрой ИРТ

Минск 2024

ВВЕДЕНИЕ

Обеспечение информационной безопасности (ИБ) играет ключевую роль в защите данных и информационных ресурсов от различных угроз и атак. ИБ включает в себя не только защиту информации и информационной инфраструктуры, но и обеспечение функционирования информационного пространства в интересах государства, граждан и организаций. Для эффективного обеспечения ИБ важны принципы системности, прочности, многоуровневой защиты, бесперебойности и благоразумности. Они направлены на создание комплексной системы защиты, способной действенно противостоять различным угрозам.

Ключевыми мерами защиты информации является контроль доступа с использованием методов идентификации, аутентификации и авторизации. Эти инструменты позволяют определить личность пользователя, установить его права доступа к информации и ресурсам, а также предотвратить несанкционированный доступ. Кроме того, аудит информационных систем играет важную роль в обеспечении безопасности данных, позволяя выявлять уязвимости и проблемы в текущем состоянии информационных технологий.

Обеспечение информационной безопасности требует комплексного подхода и постоянного совершенствования мер защиты, учитывая разнообразие угроз современного цифрового мира. Внедрение современных технологий и строгий контроль за доступом к информации существенно снижают риск утечки данных и нанесения ущерба информационным ресурсам.

Информационная безопасность (ИБ) – это важный аспект современного общества, в котором информация играет ключевую роль. ИБ заключается в обеспечении недопустимости нанесения ущерба объектам безопасности, связанным с информацией и информационной инфраструктурой. ИБ охватывает множество аспектов, включая защиту информационного пространства, информации, инфраструктуры, экономической и финансовой составляющих. Ключевым свойством ИБ является защищенность, включающая активную и пассивную защиту.

Активная защита направлена на предотвращение несанкционированного доступа к информации и защиту личных данных, эксплуатацию средств ИБ, объектов критической инфраструктуры и международные интересы. Пассивная защита, в свою очередь, способствует общественному и экономическому развитию, включая свободу обращения информации, развитие культуры, онлайн-демократии, экономики, ИТ-сектора и международное сотрудничество.

Обеспечение ИБ позволяет эффективно бороться с информационной преступностью, предотвращая незаконные действия в отношении данных, нарушение порядка доступа к информации и воздействие на средства обработки информации.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

Актуальность темы исследования подчеркивается несколькими важными аспектами. В современном мире информационная безопасность (ИБ) приобретает все большее значение из-за растущего объема и значимости данных, которые обрабатываются и хранятся в цифровом виде. Существует множество угроз, связанных с несанкционированным доступом, кражей, изменением и уничтожением информации. Эти угрозы могут нанести существенный ущерб не только отдельным организациям, но и государственным структурам и обществу в целом.

Исследование информационной безопасности становится все более важным на фоне ускоряющейся цифровизации различных сфер жизни, включая экономику, государственное управление, здравоохранение, образование и другие области. Появление новых технологий, таких как интернет вещей, искусственный интеллект и большие данные, создает новые вызовы для обеспечения безопасности информации.

Кроме того, возрастают требования к защите персональных данных, что связано с ужесточением законодательства в этой области и повышенным вниманием общественности к вопросам конфиденциальности. Введение и соблюдение международных стандартов и норм информационной безопасности становятся важными для обеспечения надежной защиты информации и данных, что способствует разработке и совершенствованию национальных политик и практик информационной безопасности.

Степень разработанности проблемы

Тема данного исследования не является новой, так как исследования в области информационной безопасности проводятся на протяжении нескольких десятилетий и охватывают как теоретические, так и практические аспекты защиты информации. Государственные органы и организации обязаны руководствоваться положениями Концепции ИБ в своей деятельности, что включает разработку нормативных правовых актов, государственных программ и планов работы, направленных на обеспечение информационной безопасности.

Цель и задачи работы

Целью данной магистерской диссертации является анализ моделей информационной безопасности, а также технических требований по вопросам ИБ.

Для достижения поставленных целей необходимо было решить следующие задачи:

1. Провести обзор литературы и практических решений в сфере информационной безопасности;

2. Выделить информацию о методах защиты информации и моделях информационной безопасности;

3. Выделить информацию о построении комплексных моделей ИБ;

4. Изучить законодательную часть касаемо моделей ИБ;

5. Провести анализ собранной информации;

6. На основе полученных результатов сформулировать методические рекомендации по построению комплексной модели информационной безопасности.

Область исследования

Основными объектами исследований являются методы защиты информации, правовые модели информационной безопасности и построение моделей информационной безопасности.

Теоретическая и методологическая основа исследования

В основу диссертации легли работы белорусских и зарубежных ученых в области защиты информации, а также были проанализированы законодательные аспекты данной темы.

Информационная база исследования сформирована на основе литературы, открытой информации, технических нормативно-правовых актов, сведений из электронных ресурсов, а также материалов научных конференций и семинаров.

Научная новизна

Данная работа заключается в анализе моделей информационной безопасности, технических требований по вопросам информационной безопасности и последующей формулировке методических рекомендаций к построению комплексной модели информационной безопасности.

Теоретическая значимость диссертации заключается в том, что в ней проведен анализ и предложены рекомендации по построению комплексной модели информационной безопасности.

Практическая значимость диссертации состоит в том, что на основе предложенных рекомендаций имеется возможность построения моделей информационной безопасности, например, в учреждении среднего образования. Подобная модель будет удовлетворять всем требованиям как с технической, так и с законодательной стороны. Так же результаты данного исследования могут быть применены в текущей системе для оценки защищенности и соответствия законодательным актам.

Основные положения, выносимые на защиту

1. Анализ моделей информационной безопасности: классификация, программные и аппаратные средства.

2. Рассмотрение процесса построения комплексной модели информационной безопасности.

3. Рассмотрение законодательных требований и рекомендаций к технологиям и методам, используемым при построении моделей.

4. Методические рекомендации к построению комплексной модели информационной безопасности на примере учреждения общего среднего образования.

Апробация диссертации и информация об использовании ее результатов

Теоретические результаты диссертационных исследований представлены в виде тезисов на следующих научных конференциях:

– 59-ой конференции аспирантов, магистрантов и студентов БГУИР, Минск, 17 – 21 апреля 2023 г;

– 60-ой конференции аспирантов, магистрантов и студентов БГУИР, Минск, 17 – 21 апреля 2024 г;

– XVII Международная научно-практическая конференция, Минск, 16 мая 2024 г.

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликовано 3 печатных работ в сборниках: 59-я конференция аспирантов, магистрантов и студентов БГУИР, 60-ой конференции аспирантов, магистрантов и студентов БГУИР, XVII Международная научно-практическая конференция БГЭУ.

Структура и объем работы

Работа состоит из введения, общей характеристики работы, трёх глав и заключения, библиографического списка. Общий объем диссертации − 66 страниц. Работа содержит 3 рисунка. Библиографический список включает 49 наименования.

В первой главе были рассмотрены классификация методов защиты информации, аппаратные и программные средства защиты информации, их особенности. Кроме того, были рассмотрены концептуальная, математическая и функциональная модели информационной безопасности. В завершении первой главы были рассмотрены правовые модели информационной безопасности.

Во второй главе была рассмотрена инфраструктура комплексной модели информационной безопасности, её основные компоненты. Помимо этого, были рассмотрены административно-организационные и нормативно-правовые аспекты построения ИБ.

В третьей главе были приведены административно-правовые рекомендации по построению ИБ, а также на основании проведенного ранее анализа информации сформулированы методические рекомендации по аппаратно-программному построению ИБ.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** рассмотрено современное состояние проблемы информационной безопасности, указаны основные определения, виды защиты информации, принципы обеспечения информационной безопасности.

В **общей характеристике работы** степень разработанности проблемы, сформулированы цель и задачи диссертации, обозначена область исследований, научная (теоретическая и практическая) значимость исследований, а также апробация работы.

В первой главе рассматривается классификация методов защиты информации, в том числе аппаратные и программные средства ЗИ, их применимость.

Аппаратные методы защиты информации могут быть реализованы на уровне аппаратных компонентов и устройств, таких как процессоры, модули аутентификации, криптографические устройства и другие специализированные элементы системы. Они обеспечивают физическую защиту данных и сетей, а также выполняют функции аутентификации, шифрования и контроля доступа.

Программные методы защиты информации могут быть реализованы на разных уровнях системы, включая операционные системы, прикладное программное обеспечение и сетевые устройства. Они включают в себя различные средства и механизмы, такие как антивирусные программы, брандмауэры, системы обнаружения вторжений, программное шифрование и многое другое.

Помимо этого, рассматривается один из самых важных методов защиты – антивирусные программы, которые могут быть реализованы на разных уровнях системы, включая операционные системы, прикладное программное обеспечение и сетевые устройства. Они включают в себя различные средства и механизмы, такие как антивирусные программы, брандмауэры, системы обнаружения вторжений, программное шифрование и многое другое.

Также рассматриваются концептуальные, функциональные и математические модели ИБ.

Концептуальная модель информационной безопасности включает определение объекта защиты, киберугроз, источников данных и методов защиты. Эта модель обычно состоит из двух уровней: сервисного и организационно-управленческого.

Математическая и функциональные модель на прямую связаны друг с другом. Математическая модель представляет собой формализованное описание сценариев в виде логических алгоритмов представленных последовательностью действий нарушителей и ответных мер. Расчетные количественные значения параметров модели характеризуют функциональные зависимости, описывающие процессы взаимодействия нарушителей с системой защиты и возможные результаты действий. Именно такой вид модели чаще всего используется для количественных оценок уязвимости объекта, построения алгоритма защиты оценки рисков и эффективности принятых мер.

Во второй главе были сделаны выводы по содержимому первой главы, на основании которых было сформулировано представление, что инфраструктура информационной безопасности включает в себя комплекс системных и организационных компонентов, предназначенных для защиты информационных ресурсов в организации. Это инфраструктура состоит из технических средств, процессов, политик и практик, которые совместно работают для защиты информации от различных угроз и уязвимостей.

Технические средства включают аппаратные и программные компоненты, такие как межсетевые экраны (firewalls), системы обнаружения и предотвращения вторжений (IDS/IPS), системы аутентификации и авторизации, системы шифрования данных, а также системы резервного копирования и восстановления. Все эти элементы обеспечивают защиту информационных ресурсов от несанкционированного доступа и кибератак.

Организационные компоненты включают политики, процедуры и стандарты, регулирующие безопасное использование информационных ресурсов. Это может включать разработку политики безопасности информации, управление доступом и аутентификацией, регулярные аудиты безопасности и обучение сотрудников. Политика безопасности информации определяет общие принципы и требования, такие как использование паролей, ограничение физического доступа и применение шифрования при передаче данных. Управление доступом и аутентификация включают процедуры и механизмы, которые определяют, кто и как может получить доступ к информационным ресурсам. Механизмы мониторинга и анализа включают системы для постоянного наблюдения за сетью, регистрацию событий и анализ безопасности. Эти механизмы позволяют обнаруживать и реагировать на угрозы и аномальную активность в реальном времени.

Физическая безопасность также является важным аспектом и включает меры

по защите физического доступа к информационным ресурсам, такие как видеонаблюдение, системы контроля доступа и ограничение доступа к серверным помещениям.

Кроме того, инфраструктура информационной безопасности включает управление уязвимостями, что подразумевает процесс идентификации, классификации и устранения уязвимостей, включая сканирование уязвимостей, патчинг и обновление программного обеспечения. Обеспечение бизнес-континуитета включает разработку планов и механизмов для восстановления после инцидентов, таких как резервное копирование данных и аварийные планы.

Для обеспечения эффективной инфраструктуры информационной безопасности применяются международные стандарты, такие как ISO/IEC 27001 и NIST Cybersecurity Framework, которые устанавливают требования и рекомендации по управлению информационной безопасностью. Инфраструктура также должна включать механизмы для мониторинга и обработки информационных инцидентов, что включает системы обнаружения инцидентов, сетевой мониторинг и процедуры реагирования на инциденты.

В третьей главе рассматриваются методические рекомендации по аппаратно-программному построению информационной безопасности (ИБ), разнообразие и количество средств защиты информации. Они подразделяются на три основные категории: физические, аппаратные и программные средства защиты. Выбор конкретных технических мер для организации зависит от региональной концепции информационной безопасности, которая определяет, что и как необходимо защищать.

Для построения системы защиты информации с использованием технических средств следует учитывать несколько принципов. Во-первых, важно использовать только лицензированное программное обеспечение, что гарантирует его надежность и безопасность. Все программные компоненты системы должны быть совместимы друг с другом, что обеспечивает их бесперебойное взаимодействие. Управляемость и легкость администрирования системы также имеют первостепенное значение, поскольку это минимизирует необходимость в сторонней технической поддержке. Кроме того, необходимо протоколировать и документировать все действия пользователей, касающиеся конфиденциальной информации, а также фиксировать случаи несанкционированного доступа. Затраты на организацию защиты информации должны быть соразмерны потенциальному ущербу от утечек или атак.

Физические средства защиты включают механические, электрические и электронные механизмы, которые работают независимо от информационных систем и создают препятствия для доступа к ним. К ним относятся замки, экраны и жалюзи, системы контроля и управления доступом (СКУД), системы видеонаблюдения и датчики движения или электромагнитного излучения. Эти средства физически

ограничивают доступ к защищаемым помещениям и фиксируют попытки несанкционированного проникновения.

Аппаратные средства защиты информации представляют собой устройства, затрудняющие несанкционированный съем информации и помогающие обнаружить потенциальные каналы утечки. Существует множество технических каналов утечки информации, включая акустические, виброакустические, оптико-электронные и электромагнитные импульсы. Для борьбы с утечками используются различные устройства, такие как генераторы шума, сетевые фильтры и сканирующие радиоприемники. Однако в обычной деятельности образовательных организаций наиболее актуальны меры против просмотра информации с экранов дисплеев, прослушивания переговоров и других подобных угроз. Для этого можно использовать физические средства защиты, а также организационные мероприятия, такие как правильное расположение мониторов и блокировка рабочих станций при оставлении рабочего места.

Программные средства защиты информации включают широкий спектр ПО, предназначенного для обеспечения информационной безопасности. Это самая многочисленная группа средств, охватывающая операционные системы, антивирусные программы, программы резервного копирования, прикладные программы с разграничением прав пользователей, программные межсетевые экраны, прокси-серверы, системы обнаружения и предотвращения вторжений, системы контроля съемных носителей и DLP и SIEM системы.

Операционные системы предлагают встроенные решения по защите конфиденциальной информации, такие как аутентификация по паролю, смарт-карте или сертификату, ограничение прав доступа и встроенные брандмауэры. Антивирусные программы выполняют функции управления доступом к съемным устройствам, оповещают о уязвимостях и обеспечивают удаленную установку и удаление программ. Программы резервного копирования, как встроенные, так и сторонние, такие как Acronis, обеспечивают сохранность данных. Прикладные программы реализуют разграничение прав пользователей через пароли и роли, а межсетевые экраны фильтруют сетевой трафик, предотвращая несанкционированный доступ.

Прокси-серверы выполняют роль посредника между пользователем и запрашиваемым интернет-ресурсом, повышая безопасность сети и экономя трафик через кэширование. Системы обнаружения и предотвращения вторжений (IDS и IPS) анализируют данные, передаваемые по сети, и блокируют подозрительные активности, что является дополнением к межсетевым экранам и антивирусам.

Системы контроля съемных носителей предотвращают несанкционированное копирование конфиденциальной информации на USB-устройства, а DLP и SIEM системы находятся на вершине программных средств защиты. DLP системы

предотвращают передачу конфиденциальной информации за пределы организации, а SIEM системы анализируют информацию от различных систем безопасности, выявляя и регистрируя инциденты ИБ, предоставляя доказательную базу для внутренних расследований и судебных разбирательств.

Далее был приведен ряд законодательных документов, среди которых в том числе Концепция информационной безопасности Республики Беларусь. Была принята 2019 году, дополняет Конституцию и Концепцию национальной безопасности. Этот документ регулирует меры защиты информации, виды и источники угроз, и первоочередные мероприятия по обеспечению ИБ. Государственные органы и организации должны руководствоваться положениями Концепции ИБ, которая также служит основой для разработки нормативных актов и программ в области ИБ, обеспечивая правовое положение субъектов и регулируя деятельность государственных органов. Государственная политика в этой сфере основывается на принципах соблюдения законодательства, правового равенства участников информационного взаимодействия, приоритетного развития отечественных технологий, и обеспечивает баланс интересов личности, общества и государства.

Для учреждений общего среднего образования разработаны рекомендации по выполнению первоочередных мер по информационной безопасности. В каждом учреждении необходимо назначить ответственного за защиту информации, проводить его регулярное обучение и организовать работу по защите информации. Это включает определение границ информационной системы (ИС), категорирование информации, отнесение ИС к классу типовых систем, и внедрение технических, криптографических и организационных мер защиты. Система защиты информации должна быть сертифицирована, и при необходимости, для создания и аттестации системы защиты могут привлекаться специализированные организации. Эти меры направлены на обеспечение безопасной обработки персональных данных и защиту информации в образовательных учреждениях.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1 Проведен анализ различных моделей и подходов к обеспечению информационной безопасности. Были выделены и классифицированы основные методы защиты информации, включая как технические, так и организационные аспекты. Осуществлен обзор существующих аппаратных и программных средств защиты информации с акцентом на их эффективность и применимость в различных условиях.

2 Рассмотрена типовая организация инфраструктуры ИБ, проанализированы технические и организационные компоненты для защиты данных. Приведены основные сведения нормативно-правовых методов построения ИБ.

3 Представлены практические методические рекомендации по реализации комплексной модели информационной безопасности, а также рассмотрены административно-правовые рекомендации, основанные на анализе текущего законодательства и нормативных актов.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1 – Нестерович, Ю.Н. Цифровая трансформация процессов в системе образования = Digital transformation of processes in the education system / Нестерович Ю.Н. // Информационная безопасность: сборник материалов 59-й научной конференции аспирантов, магистрантов и студентов БГУИР, Минск, 17–21 апреля 2023 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2023. – С. 48–49.

2 – Нестерович, Ю.Н. О нормативно-правовом обеспечении информационной безопасности учреждений общего среднего образования = On the regulatory and legal provision of information security of general secondary education institutions / Нестерович Ю.Н. // Информационная безопасность: сборник материалов 60-й юбилейной научной конференции аспирантов, магистрантов и студентов БГУИР, Минск, 23–24 апреля 2024 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2024.

3 – Нестерович, Ю.Н. О нормативно-правовом обеспечении информационной безопасности учреждений общего среднего образования // Экономический рост Республики Беларусь: глобализация, инновационность, устойчивость: материалы XVII Международной научно-практической конференции БГЭУ, Минск, 16 мая 2024 г. / Белорусский государственный экономический университет. – Минск, 2024. – С. 356.