DOI 10.37882/2223-2966.2023.7-2.27

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ОРГАНИЗАЦИИ

Сальников Евгений Анатольевич
Доцент-практик, Финансовый университет при правительстве РФ, EASalnikov@fa.ru
Демидов Лев Николаевич
канд. техн. наук, доцент, доцент, Финансовый университет при правительстве РФ, LDemidov@fa.ru

Аннотация. Данная статья посвящена исследованию методов и систем защиты информации в организации. Цель работы заключается в анализе и описании современных методов и систем защиты информации, их эффективности и применимости в современных условиях, а также разработка новых подходов к обеспечению безопасности данных в организации.
Для достижения поставленной цели были использованы методы анализа научной литературы и мнений экспертов в области информационной безопасности. Были проанализированы существующие системы защиты информации, их преимущества и недостатки, а также особенности применения в различных организациях.
Основными результатами исследования являются следующие: проанализированы основные проблемы, связанные с применением существующих систем защиты информации и предложены способы их решения; разработаны рекомендации по выбору и внедрению систем защиты информации в организации; предложены новые методы защиты информации, основанные на применении современных технологий, таких как искусственный интеллект и машинное обучение. Проведен анализ эффективности различных методов защиты, выявлены преимущества и недостатки. Предложена концептуальная модель информационной безопасности. Также в статье особое внимание уделяется применению методов и систем защиты в конкретных условиях и требованиях организации.

Ключевые слова: информационная безопасность, системы защиты информации, криптографические алгоритмы, межсетевые экраны, системы идентификации и аутентификации, биометрические технологии, системы контроля доступа, аудит безопасности.

METHODS AND SYSTEMS OF INFORMATION PROTECTION IN THE ORGANIZATION

E. Salnikov
L. Demidov

Summary: This article is devoted to the study of methods and systems of information protection in the organization. The purpose of the work is to analyze and describe modern methods and information security systems, their effectiveness and applicability in modern conditions, as well as to develop new approaches to ensuring data security in an organization.
To achieve this goal, methods of analyzing scientific literature and opinions of experts in the field of information security were used. The existing information security systems, their advantages and disadvantages, as well as the features of application in various organizations were analyzed.
The main results of the study are as follows: the main problems associated with the use of existing information security systems are analyzed and ways to solve them are proposed; recommendations were developed for the selection and implementation of information security systems in the organization; new methods of information protection based on the use of modern technologies such as artificial intelligence and machine learning are proposed. An analysis of the effectiveness of various protection methods was carried out, advantages and disadvantages were identified. A conceptual model of information security is proposed. Also in the article, special attention is paid to the application of methods and systems of protection in the specific conditions and requirements of the organization.

Keywords: information security, information security systems, cryptographic algorithms, firewalls, identification and authentication systems, biometric technologies, access control systems, security audit.

Введение

В современном мире информация играет огромную роль в жизни людей и организаций. Она стала ключевым ресурсом для развития бизнеса, научных исследований и государственного управления. Однако, с появлением новых технологий и развитием информационных систем, появились и новые угрозы для информационной безопасности. Несмотря на то, что многие компании вкладывают существенные средства в защиту информации, уровень защищенности все еще оставляет желать лучшего. Каждый день в мире происходят тысячи атак на информационные системы, причиняющие серьезный ущерб организациям. Современная организация хранит и обрабатывает большое количество информации, включая конфиденциальные данные о клиентах, партнерах и сотрудниках. Эта информация может стать целью для кибератак и мошенничества, что делает безопасность информации критически важной для успеха бизнеса. Поэтому, информационная безопасность является одним из ключевых аспектов для любой организации.

В современном мире информация является одним из наиболее ценных ресурсов. Компании и организации хранят большие объемы конфиденциальной информации, включая личные данные клиентов, финансовые отчеты, интеллектуальную собственность и т.д. Эта информация может стать целью киберпреступников, которые могут использовать ее для мошенничества, шпионажа или вымогательства.

Примерами нарушений информационной безопасности могут служить следующие случаи. В 2020 году ком-

пания Twitter подверглась масштабной атаке, в результате которой были скомпрометированы аккаунты многих знаменитостей и компаний, их твиты были заменены на сообщения о биткоинах. Это показало, что даже крупным компаниям, имеющим значительные ресурсы для защиты информации, угрозы кибербезопасности могут быть очень серьезными.

В 2017 году компания Equifax стала жертвой крупнейшего в истории утечки конфиденциальных данных. Были украдены личные данные более 147 миллионов человек, включая социальные страховые номера, даты рождения, имена и адреса. Это событие вызвало широкое обсуждение о необходимости повышения мер безопасности в компаниях, работающих с чувствительными данными.

Прежде чем мы перейдем к системам защиты информации, давайте рассмотрим основные типы угроз информационной безопасности, которые могут возникнуть в организации:

1. Вредоносное программное обеспечение (вирусы, черви и т.д.). Вредоносное программное обеспечение может использоваться для получения несанкционированного доступа к системе и украсть конфиденциальные данные или повредить систему.
2. Фишинг и социальная инженерия. Киберпреступники могут использовать фишинговые атаки, чтобы получить доступ к системе путем манипуляции сотрудниками организации.
3. Несанкционированный доступ. Несанкционированный доступ может быть вызван недостаточными мерами безопасности или ошибками в конфигурации системы.
4. Хакерские атаки. Хакеры могут использовать уязвимости в системе для получения несанкционированного доступа.
5. Утечки данных. Утечки данных могут произойти из-за несанкционированного доступа, ошибок сотрудников или других причин.

Таким образом, чтобы защитить информацию от несанкционированного доступа, модификации и уничтожения, необходимо использовать методы и системы защиты информации.

Методы защиты информации могут быть разделены на две категории: методы технической защиты и методы организационной защиты.

Техническая защита информации — это использование технических средств и методов для защиты информации от утечки или несанкционированного доступа. Она включает в себя следующие методы:

Криптография — это наука обеспечения конфиденциальности, целостности и аутентичности информации путем применения различных алгоритмов шифрования. Криптография широко используется для защиты информации в сетях, при передаче данных и хранении информации.

Одним из наиболее эффективных является шифрование данных. Шифрование — это процесс преобразования открытого текста в непонятный для постороннего наблюдателя. Существует множество алгоритмов шифрования, которые позволяют защитить данные от несанкционированного доступа. Шифрование может быть симметричным или асимметричным. Симметричное шифрование использует один ключ для зашифровки и расшифровки информации, в то время как асимметричное шифрование использует пару ключей — открытый и закрытый. Одним из наиболее известных алгоритмов является RSA, который основан на использовании больших простых чисел. Один из практических примеров использования шифрования — это HTTPS-протокол, который используется для защиты передачи данных между веб-сервером и веб-браузером.

Антивирусная защита — это метод защиты, который предназначен для обнаружения и удаления вредоносного программного обеспечения, такого как вирусы, трояны и шпионское ПО.

Фильтрация трафика — это метод защиты, который позволяет блокировать доступ к определенным сайтам или ресурсам, которые могут быть опасными для организации. Фильтрация трафика может быть настроена на уровне маршрутизатора или на уровне приложения. Фильтрация трафика может использоваться для защиты сети от атак DDoS, снижения риска заражения компьютеров в сети вирусами и предотвращения утечки конфиденциальной информации. Примером системы фильтрации трафика является Cisco ASA.

Организационная защита информации — это использование организационных методов для защиты информации от утечки или несанкционированного доступа. Она включает в себя следующие методы:

Обучение сотрудников — это метод защиты, который предназначен для повышения осведомленности сотрудников о безопасности информации. Обучение сотрудников может включать в себя обучение правилам использования паролей, отчетности о нарушениях информационной безопасности, а также знакомство с методами социальной инженерии, которые используются злоумышленниками для получения доступа к информации.

Управление доступом — это метод защиты, который предназначен для ограничения доступа к конфиденциальной информации только тем сотрудникам, кото-

рые должны иметь к ней доступ. Управление доступом может включать в себя применение систем управления доступом, ролевой политики, а также использование методов идентификации и аутентификации пользователей. Аутентификация позволяет убедиться в том, что пользователь, запрашивающий доступ к информации, имеет право на этот доступ. Для аутентификации могут использоваться пароли, отпечатки пальцев, смарт-карты и другие средства. Одним из практических примеров использования системы аутентификации является система двухфакторной аутентификации Google Authenticator.

Резервное копирование — это метод защиты, который предназначен для защиты информации от потери при отказе оборудования или других неожиданных событиях. Резервное копирование может включать в себя создание резервных копий данных на внешние носители, такие как жесткие диски или облако. Один из практических примеров системы резервного копирования — это Veeam Backup & Replication.

Мониторинг — это метод защиты, который предназначен для отслеживания необычной активности в сети и обнаружения возможных угроз. Мониторинг может включать в себя использование системы интеллектуального анализа поведения, которая способна обнаруживать необычную активность и отправлять оповещения сотрудникам ответственным за информационную безопасность. Например, система обнаружения вторжений позволяет обнаруживать несанкционированный доступ к системе. Она анализирует сетевой трафик и действия пользователей, и в случае обнаружения подозрительной активности отправляет уведомление администратору системы. Практический пример системы мониторинга безопасности — это система мониторинга событий Splunk. Еще одним из примеров являются системы обнаружения вторжений (IDS) предназначены для выявления несанкционированного доступа к информации. IDS могут быть разделены на две категории: системы сетевого обнаружения вторжений (NIDS) и системы обнаружения вторжений на уровне хоста (HIDS). Также еще один пример системы обнаружения вторжений — NIDS позволяющие выявлять несанкционированный доступ к информации на уровне сети. Для этого используются анализаторы сетевого трафика, которые отслеживают сетевую активность и выявляют подозрительные пакеты данных. Еще одним примером системы защиты информации может служить SIEM (Security Information and Event Management). Это интегрированная система, которая используется для мониторинга и анализа безопасности в компьютерной сети. SIEM использует логические алгоритмы, чтобы анализировать данные, собранные из различных источников, и выявляет аномальные события и потенциальные угрозы для информационной безопасности.

Системы управления информационной безопасностью организаций — это комплексное решение, которое включает в себя методы и системы защиты информации, процедуры аудита и мониторинга, а также политики и стандарты информационной безопасности. Эти системы обеспечивают надежную защиту информации, управление рисками и соблюдение соответствующих нормативных требований.

Системы управления информационной безопасностью могут включать в себя следующие компоненты:

— Политики информационной безопасности — набор правил и рекомендаций, определяющих требования к защите информации в организации. Политики могут включать в себя требования к паролям, процедуры резервного копирования данных, процедуры аудита и т.д.
— Системы мониторинга и аудита — это программные средства, которые позволяют отслеживать активности пользователей и обнаруживать потенциальные угрозы безопасности. Эти системы могут включать в себя мониторинг сетевого трафика, логирование активностей пользователей и т.д.
— Информационные системы управления безопасностью (ISMS) — это комплексные решения, которые позволяют управлять информационной безопасностью в организации. ISMS включают в себя процедуры управления рисками, процедуры управления доступом, процедуры мониторинга и аудита и т.д.
— Системы управления доступом (Access Control Systems, ACS) — это программные и аппаратные средства, которые позволяют контролировать доступ пользователей к информационным ресурсам организации. Системы управления доступом могут включать в себя авторизацию на основе паролей, биометрическую аутентификацию и т.д.

При выборе системы управления информационной безопасностью необходимо учитывать особенности организации, ее бизнес-процессы и индивидуальные требования к защите информации. Для этого необходимо провести анализ рисков и разработать соответствующие меры по защите информации.

Важным вопросом является рассмотрение различных моделей информационной безопасности, которые могут быть применены при построении системы информационной безопасности.

При создании модели информационной безопасности объектами, которые должны быть защищены, являются объекты информатизации, ресурсы информационной системы, информационные системы, информационные технологии, программные средства, сети связи, автоматизированные системы. В большинстве случаем

защищаемый объект — это носитель информации или информационный процесс.

Модели безопасности посредством системотехнического подхода, дают возможность рассмотреть решение следующих задач:

— выбор, обоснование базовых принципов архитектуры автоматизированных систем;
— подтверждение свойства защищенности системы;
— составления формальной спецификации политики безопасности разрабатываемых систем.

Существует несколько моделей, каждая из которых может ответить на поставленные вопросы.

Рассмотрим подробнее *концептуальную модель безопасности*, которая отвечает на часто задаваемые вопросы и схематично отражает общую структуру модели информационной безопасности, вокруг которой строятся другие модели и концепции информационной безопасности. Для построения концептуальной модели информационной безопасности, независимо от того, насколько проста или сложна информационная система, необходимо ответить, как минимум на три вопроса: что защищать, кого защищать и как защищать. Это минимум, и его может быть достаточно для небольших информационных систем. Однако, учитывая возможные последствия, лучше построить полную концептуальную модель информационной безопасности, для которой необходимо определить:

— Источники информации
— Приоритет или степень важности информации.
— Источники угроз
— Цели угроз
— Угрозы
— Способы доступа
— Направления защиты
— Средства защиты
— Методы защиты.

Наиболее полная концептуальная модель информационной безопасности, общая для всех информационных систем, схематично может быть представлена следующим образом (см. рис. 1).

Концептуальную модель информационной безопасности принято делить на несколько различных уровней. Во многих случаях достаточно двух уровней. Более высокий организационно-управленческий уровень, который охватывает организацию в целом и информационную систему предприятия, и более низкий сервисный уровень, который относится к отдельным подсистемам и различным сервисам самой информационной системы.

Концепции и программы верхнего уровня возглавляются лицом, непосредственно ответственным за информационную безопасность организации. В небольших организациях это, как правило, руководитель самой организации. В более крупных организациях эту ответственность несет непосредственно руководитель отдела информационных технологий или, если создан отдельный отдел информационной безопасности, руководитель этого отдела.

Программы безопасности верхнего уровня должны включать следующие стратегические цели:

1. Стратегическое планирование
2. Разработку и исполнение политики в области информационной безопасности
3. Оценка рисков и управление рисками
4. Координация деятельности в области информационной безопасности
5. Контроль деятельности в области ИБ.

Рис. 1. Концептуальная модель информационной безопасности

Основная цель или видение программы нижнего уровня заключается в обеспечении надежной и экономически эффективной защиты информационных подсистем и сервисов.

На этом уровне принимаются решения о том, какие механизмы, средства и методы защиты использовать, закупаются и устанавливаются аппаратные средства, внедряется текущий контроль, осуществляется мониторинг всей системы информационной безопасности и отслеживание слабых мест, а также проводится начальное обучение персонала.

Обычно программами нижнего уровня занимаются ответственные менеджеры по информационной безопасности, системные администраторы и менеджеры, а также менеджеры служб. Наиболее важным действием на этом уровне является оценка важности как самой службы, так и обрабатываемой через нее информации.

Таким образом, создание концептуальной модели информационной безопасности призвано дать ответы на общие вопросы и в то же время схематично отразить общую структуру модели, на которой строятся другие модели и концепции информационной безопасности. В то же время реализация концептуальной модели информационной безопасности предполагает создание нескольких уровней. Как правило — это сервисный и организационно-управленческий уровень.

Концептуальная модель определяет процесс разработки методических рекомендаций для ее реализации, которые составляют основу информационной безопасности. После разработки концептуальной модели можно построить *математическую и функциональную модель информационной безопасности*.

Математические и функциональные модели напрямую связаны между собой. Математическая модель — это структурное описание сценария в виде логического алгоритма, представленного последовательностью реакций на действия нарушителя.

Рассчитанные количественные значения параметров модели характеризуют процесс взаимодействия нарушителя и системы защиты, а также функциональные зависимости, описывающие возможные результаты действий.

Данный тип модели чаще всего используется для количественной оценки уязвимости объекта, построения алгоритмов защиты для оценки рисков и эффективности реализуемых мер.

Эти модели должны быть построены с учетом следующих ключевых соображений:

— выбор математически строгих критериев оценки оптимальности системы защиты информации для конкретной архитектуры информационной системы;
— четкая математическая формулировка задачи моделирования защиты информации, позволяющая построить защиту информации в соответствии с этими критериями с учетом заданных требований к системе защиты.

На практике очевидно, что такие численные оценки невозможно провести без использования методов математического моделирования, поскольку мы сталкиваемся с многочисленными рисками угроз безопасности.

В зависимости от целей и решаемой проблемы можно построить ряд математических моделей и применить их к информационной безопасности на этапе проектирования системы информационной безопасности для оценки ее эффективности.

Перед разработкой и внедрением любой модели необходимо обратить внимание на следующие свойства:

— Ограниченность. Любая модель отражает только те свойства, которые необходимы для решения поставленной в модели задачи с определенной степенью точности. Поэтому важно знать границы применимости модели и способы работы с ней. Эти свойства характеризуют достаточность модели для решения задачи.
— Итеративность. Любая модель представляет только те свойства моделируемой системы, которые известны создателю модели. Если появляются новые, ранее неизвестные характеристики, модель должна быть модифицирована (не обязательно подразумевает изменение). Эта характеристика подразумевает, что модель должна быть изменена для решения проблемы.

Таким образом еще одним важным вопросом при построении модели информационной безопасности или системы является их жизненный цикл, который включает следующие этапы (см. рис. 2).

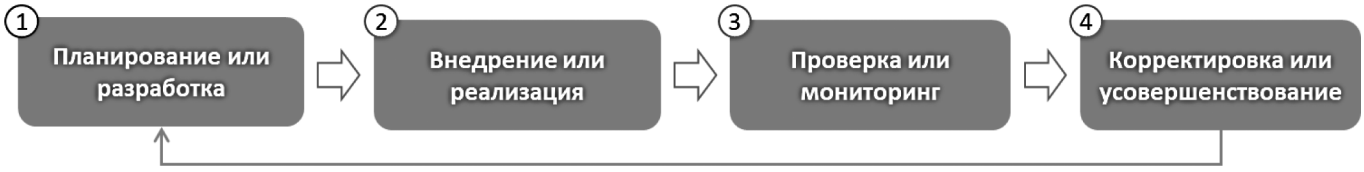

Рис. 2. Жизненный цикл модели безопасности

Конечно, недостаточно просто построить систему информационной безопасности, применяя различные модели; необходимо соблюдать жизненный цикл этой системы. Важно не упустить ни одного важного момента. Это обеспечит минимальный (базовый) уровень информационной безопасности, который является обязательным для любой информационной системы.

Практические примеры

Рассмотрим несколько примеров использования систем защиты информации в реальных компаниях.

— JPMorgan Chase — один из крупнейших банков в США — использует множество систем защиты информации, чтобы предотвратить угрозы информационной безопасности. Компания использует систему обнаружения вторжений, которая позволяет отслеживать подозрительную активность в системе, а также множество систем аутентификации и шифрования для защиты конфиденциальных данных клиентов.

— Google — одна из крупнейших компаний в мире, которая хранит огромное количество информации о своих пользователях. Компания использует множество систем защиты информации, включая системы мониторинга, которые позволяют обнаруживать подозрительную активность, и системы аутентификации, которые обеспечивают безопасный доступ к данным.

— Lockheed Martin — американская компания, которая занимается разработкой и производством изделий в области аэрокосмической и оборонной промышленности. Компания использует множество систем защиты информации, включая системы мониторинга и системы аутентификации, а также системы защиты от внешних угроз, такие как DDoS-атаки.

— Apple — крупнейший производитель электроники, хранящий огромное количество конфиденциальной информации о своих пользователях. Компания использует множество систем защиты информации, включая системы мониторинга и аутентификации, а также шифрование данных, чтобы предотвратить доступ к конфиденциальной информации.

— Target — крупнейшая американская розничная сеть — стала жертвой одного из самых серьезных нарушений информационной безопасности в истории. В 2013 году хакеры получили доступ к базе данных, содержащей информацию о 40 миллионах клиентов Target. В результате компания потеряла миллионы долларов и подверглась сильной критике со стороны общественности. Этот инцидент подчеркивает важность систем защиты информации и показывает, что даже крупные компании могут стать жертвами кибератак.

В качестве практических примеров можно привести реализацию системы защиты информации в банковской сфере. Банки используют множество методов и систем защиты информации, чтобы защитить своих клиентов от мошенников и несанкционированного доступа к их финансовым средствам. Например, при доступе к интернет-банкингу клиента требуется ввести логин и пароль, после чего на мобильный телефон клиента отправляется код подтверждения. Также банки могут использовать системы обнаружения вторжений, чтобы защитить свои сети от хакерских атак.

Еще одним примером может служить компания, которая занимается разработкой программного обеспечения. Компания может использовать шифрование данных для защиты их кода программы от несанкционированного использования. Также они могут использовать системы контроля доступа, чтобы ограничить доступ к их разработкам только для авторизованных пользователей.

Перспективы защиты информации

Современные организации находятся под постоянным воздействием угроз информационной безопасности, таких как кибератаки, вирусы, трояны и многие другие. Информационная безопасность становится все более важной для организаций, поскольку любые нарушения безопасности могут привести к серьезным последствиям, таким как потеря конфиденциальной информации, нарушение бизнес-процессов, штрафы и репутационный ущерб.

В свете этих угроз организации постоянно ищут новые методы и системы защиты информации. В будущем методы и системы защиты информации будут становиться все более сложными и интегрированными, чтобы противостоять новым и более утонченным угрозам.

Системы защиты информации будут включать в себя множество технологий, таких как защита от вирусов и других вредоносных программ, защита от кибератак, шифрование данных, управление доступом и многое другое. Важно отметить, что системы защиты информации не ограничиваются только техническими методами, такими как защита от вирусов и кибератак, но также включают в себя управление рисками, обучение сотрудников и управление процессами.

Заключение

Информационная безопасность является одним из важнейших аспектов в управлении информационными технологиями в современных организациях. В статье рассмотрены основные методы и системы защиты информации, такие как шифрование данных, авторизация

и аутентификация пользователей, системы обнаружения вторжений и системы управления информационной безопасностью. Для обеспечения надежной защиты информации необходимо использовать комплексный подход, который включает в себя применение нескольких методов и систем защиты. Кроме того, необходимо проводить регулярный анализ рисков и обновлять системы защиты, чтобы минимизировать возможность возникновения угроз безопасности. Важно отметить, что методы и системы защиты информации не являются универсальными и должны выбираться и настраиваться индивидуально для каждой организации в зависимости от ее особенностей и потребностей.

Информационная безопасность является важной темой для организаций любого масштаба и является неотъемлемой частью успешной работы. Несоблюдение мер безопасности может привести к серьезным последствиям, таким как утечки данных, нарушение правил конфиденциальности и репутационный ущерб. Успешные применения информационных средств на практике показывают, что использование этих методов и систем может эффективно защитить информационные ресурсы организации от угроз и утечек данных.

Для обеспечения эффективной защиты информации необходимо использовать комплексный подход, включающий в себя как технические, так и организационные меры, а также регулярно проводить анализ рисков и обновлять системы защиты. Приведенные практические примеры, которые показывают, что системы защиты информации являются неотъемлемой частью бизнес-стратегии в настоящее время.

В будущем, они будут становиться все более сложными и интегрированными, чтобы противостоять новым и более утонченным угрозам. Организации должны постоянно совершенствовать свои методы и системы защиты информации, чтобы уменьшить риски и защитить свои активы.

ЛИТЕРАТУРА

1. Богомолова, Л.И. Организационная защита информации в организации / Л.И. Богомолова // Информационные технологии и вычислительные системы. — 2016. — № 2. — С. 32–39.
2. Семенов, А.И. Применение систем управления доступом для защиты конфиденциальной информации / А.И. Семенов // Компьютерные сети и информационная безопасность. — 2015. — № 1. — С. 45–50.
3. Павлова, О. Организационные аспекты информационной безопасности предприятия. М.: Издательство «Лань», 2019.
4. Миронов, А. Информационная безопасность предприятий: защита информации и борьба с киберугрозами. М.: Издательство «Проспект», 2020.
5. Cavelty, Myriam Dunn; Mauer, Victor (2016). "Cybersecurity in Switzerland". Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense. Springer International Publishing. pp. 305–329.
6. Kizza, J.M. (2016). Guide to computer network security. Springer.
7. Pfleeger, C.P., & Pfleeger, S.L. (2015). Security in computing. Pearson.
8. CIS Controls. Center for Internet Security. https://www.cisecurity.org
9. Symantec. (2021). Security Center. https://www.symantec.com
10. Google. (2021). Google Authenticator. https://support.google.com
11. Splunk. (2021). Security Information and Event Management (SIEM). https://www.splunk.com/
12. Veeam. (2021). Backup & Replication. https://www.veeam.com

Журнал «Современная наука: актуальные проблемы теории и практики»