**УДК 004**

***Синцов Юрий Юрьевич***
***студент магистратуры***
***кафедра Прикладная математика и информатика,***
***Институт математики, физики и информационных технологий,***
***Тольяттинский государственный университет,***
***Россия, г. Тольятти***
***e-mail: yuriytch@yandex.ru***

# РАЗРАБОТКА И ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПОМОЩЬЮ СОВРЕМЕННЫХ СРЕДСТВ ЗАЩИТЫ

***Аннотация:*** *Статья раскрывает особенности разработки современных средств защиты информации. Анализируются такие средства защиты информации, как физические средства, аппаратные, криптографические средства защиты информации.*

**Ключевые слова:** информационная система, безопасность, аппаратные, программные средства защиты, криптография.

***Sintsov Yuri Yurievich***
***master student***
***Department of Applied Mathematics and Computer Science***
***Institute of Mathematics, Physics and Information Technology***
***Togliatti State University,***
***Russia, Togliatti***

# DEVELOPMENT AND PROVISION OF INFORMATION SECURITY WITH THE HELP OF MODERN MEANS OF PROTECTION

***Abstract:*** *The article discloses the features of the development of an information system for personnel accounting in a system with which you can view information, track changes about any organization based on a personnel database, receive the necessary inquiries and analytical reports, and make decisions based on the information received.*

**Key words:** information system, security, hardware, software protection, cryptography.

Почему важно защищать информацию? Информация в современном мире является крайне важным ресурсом и инструментом. С ее помощью ведутся войны, проводятся избирательные компании и заключаются многомиллионные

контракты. В нашем веке информационных технологий информация играет очень важную роль. Неправомерное искажение или фальсификация, любое повреждение или разглашение определенной части информации, равно как и дезорганизация процессов ее обработки и передачи в информационно-управляющих системах наносят серьезный материальный и моральный урон многим субъектам, участвующим в процессах автоматизированного информационного взаимодействия [1] . Именно поэтому очень важно защищать ее.

Непрерывный процесс обеспечения информационной защиты в компании, основан на методах контроля как внешних так и внутренних потоков информации, организации и реализации мер по поддержке надёжного функционирования локальной сети и серверного оборудования, предотвращения утечек информации. В зависимости от конкретной информационной структуры компании формируется свод правил и нормативных документов, составляющих политику информационной безопасности в которой учитываются и регламентируются действия сотрудников по обеспечению безопасности, использование технических и программных средств защиты информации, систем предотвращения несанкционированного доступа как к информации, так и к физическому оборудованию. В настоящее время система обеспечения информационной безопасности становятся одной из обязательных характеристик любой компании.

Попробуем рассмотреть комплекс инженерно-технической защиты, состоящий из:

•Физических средств защиты;

•Аппаратных средств защиты;

•Программной защиты информации;

•Криптографических средств защиты;

К физическим средствам защиты можно отнести разнообразные приспособления, конструкции, изделия, и прочие устройства для создания барьеров на пути злоумышленников. К подобным средствам защиты относятся

устройства любого типа, воспрещающие несанкционированный доступ и других несущих вред действий. Подобные средства применяются для охраны территории предприятия, зданий, помещений, оборудования, продукции и финансов, а также для наблюдения за ними. Особо нужно выделить контроль доступа в охраняемые здания и помещения. Все подобные средства защиты можно разделить на следующие группы:

— охранные и охранно-пожарные системы;

— охранное телевидение;

— охранное освещение;

— средства физической защиты».

Аппаратные средства защиты информации включают в себя разного рода технические устройства, созданные для защиты информации от разглашения, утечки и несанкционированного доступа. Их использование позволяет решать задачи проведения специальных исследований технических средств на наличие возможных каналов утечки информации, их локализации, способствует обнаружению средств промышленного шпионажа, предотвращает доступ к конфиденциальной информации [2]. Классифицируются на средства обнаружения устройств съема информации и исследования каналов утечки, средства активного и пассивного противодействия. Аппаратные средства и методы защиты распространены очень широко, однако при раскрытии принципов действия могут потерять большую часть своей актуальности.

Программные средства защиты информации от несанкционированного доступа реализуют следующие принципы информационной безопасности:

- идентификация субъектов и объектов;

- разграничение доступа к вычислительным ресурсам и информации;

- контроль и регистрация действий с информацией и программами.

Самым популярным методом идентификации является парольная идентификация. Следует учитывать, что пароль можно перехватить, подслушать или подсмотреть и даже угадать. Поэтому обязательным фактором безопасности

должна являться система регулярной смены и использования паролей достаточной сложности.

Актуальным направлением программных средств является защита от копирования. Средства защиты от копирования предотвращают нелегальное копирование информации и программного обеспечения и в настоящее время, являются единственно надежным средством, которое защищает авторское право разработчиков. Под средствами защиты от копирования понимаются средства, обеспечивающие выполнение программой своих функций только при опознании некоторого уникального некопируемого элемента. Таким элементом может быть определенная часть программного кода или специальное устройство.

С развитием и усложнением компьютерных технологий, увеличением объёмов используемой информации развивается и направление защиты информации от разрушения. Причины разрушения информации весьма разнообразны и связаны как с аппаратными, так и с субъективными причинами. Зачастую привычных средств резервного копирования или распределённого хранения критически важной информации, особенно в крупных кампаниях, становится недостаточно или экономически неэффективно. Решение этой проблемы привело к росту специализированных центров обработки данных (ЦОД), гарантирующих как сохранность, так и конфиденциальность, достаточность места для работы с большими объёмами информации.

Важная часть инженерно-технической защиты - криптографические средства. Это специальные математические средства защиты информации, передаваемой по интернет-сети и обрабатываемой на ЭВМ с использованием разнообразных методов шифрования [3]. Криптографические методы занимают почти самое важное место и выступают самым надежным средством обеспечения защиты информации на длительные периоды.

Среди достоинств криптографических методов защиты следует отметить высокий уровень защиты данных, экономичность в реализации и эффективность в быстродействии.

Недостатком криптографических методов защиты является сложность в реализации, что требует привлечение специалистов по криптографии для обеспечения требуемого уровня защиты данных.

Криптографические методы относятся к программному комплексу защиты информации, но в тенденциях современного бизнеса это направление становится все актуальнее. Так как вся отчетность и многие торговые операции в связи с улучшением информационных технологий переходят на электронный документооборот, и подлинность документов и подписей необходимо подтверждать, а также защищать документы от правки или доступа к ним посторонних лиц, то криптография, как метод защиты информации, становится необходимым методом в политике информационной безопасности.

**Список литературы:**

1. Расторгуев С.П. Основы информационной безопасности: учеб. пособие для вузов. М.: Academia, 2020. 186 с.

2. Саак А.Э. Информационные технологии управления: учеб. для вузов. М.: Питер, 2018. 318 с.

3. Баричев С.Г, Серов Р.Е. Основы современной криптографии: учебное пособие. М.: Горячая линия, Телеком, 2018. 175 с.