**Введение**

Защита информации всегда была и остается актуальной ввиду ее важности в различных сферах жизни человека, начиная от желания защитить свои личные тайны, заканчивая необходимостью защиты интересов целого государства.

Во все времена главной опорой для действующей власти и успехом в ведении войн была надежная и эффективно действующая связь. В то же время все, кто был заинтересован в этой самой связи, осознавали что произойдет, если их передаваемая информация попадет не в те руки, если враждебному государству станут известны важные секреты. Именно беспокойство за то, что недоброжелатели перехватят сообщение, послужило толчком к активному развитию шифрования как способа сокрытия содержания сообщения таким образом, чтобы доступ к нему мог иметь только тот, кому оно предназначено.

Шифрование — это единственная возможность защитить нашу личную жизнь и гарантировать успешное функционирование цифрового рынка. Искусство секретной тайной связи, также известное как криптография, дает вам замки и ключи в век информационных технологий. Правда в том, что растущая необходимость общества в криптографии вступает в противовес требованиям органов безопасности государства. Долгое время полиция и специальные службы осуществляли контроль телефонных переговоров для получения улик против преступников и террористов, однако создание сверхстойких способов шифрования угрожает их ценности. В связи со вступлением в новый двадцать первый век, защитники гражданских прав добиваются массового использования криптографии для защиты прав человека на неприкосновенность личной жизни. Вместе с этим представители бизнеса, которым также необходима стойкая защита, обеспечивающая безопасности проводимых сделок, которые повсеместно осуществляются в стремительно развивающемся мире цифровой экономики. Вместе с этим представители правопорядка различных стран оказывают давление на правительства, добиваясь ограничения на использование криптографии. Из-за этого возникает вопрос выбора между правом на личную жизнь и эффективно действующей полицией, так как достижение компромисса в этой проблеме крайне сложно.

Вместе с тем, что сегодня криптография оказывает большое влияние на действия простых людей, также нельзя не сказать и то, что военная криптография остается приоритетным и важным вопросом. Здесь хочется добавить и то, что Первая мировая война считается “войной химиков” из-за того, что были впервые применены такие вещества как иприт и хлор. Вторая мировая война в свою очередь называется “войной физиков”, в связи с взрывом атомной бомбы. Таким же образом считают, что третья мировая война будет называться “войной математиков”, так как математики будут контролировать важнейшее оружие нашего времени — информацию.

Из-за того, что именно математиками создаются шифры, которые в дальнейшем используются в военных целях, эти же математики играют главную роль, когда дело доходит до взлома уже вражеских шифров.

Говоря о начале применения первых шифрующих устройств, стоит упомянуть сциталу. Она впервые появилась в описании древнегреческого поэта Архилоха, жившего в 7 веке до н.э. Сцитала - это устройство, состоящее из двух одинаковых по толщине палок, которые и назывались сциталами и находились у собеседников. Для использования сциталы необходимо было плотно намотать на нее узкую полосу папируса, а затем нанести на нее текст сообщения. После этого полосу снимали и передавали другому собеседнику, которому оставалось только намотать папирус на сциталу и прочитать текст. Однако древнегреческим философом Аристотелем был придуман, метод обхода защиты сциталы. Философ предложил наматывать перехваченный пергамент на длинный конус. Таким образом, в определенном месте текст сообщения начинал приобретать смысл, тем самым можно было определить секретный ключ – диаметр сциталы, а значит, и расшифровать секретное послание.

Наиболее известным и близким к современности является следующий пример – шифровальная машина “Энигма”, которая получила широкую известность из-за использования ее во время Второй мировой войны силами [гитлеровской Германии](https://ru.wikipedia.org/wiki/%D0%93%D0%B8%D1%82%D0%BB%D0%B5%D1%80%D0%BE%D0%B2%D1%81%D0%BA%D0%B0%D1%8F_%D0%93%D0%B5%D1%80%D0%BC%D0%B0%D0%BD%D0%B8%D1%8F). По аналогии с другими роторными машины, «Энигма» состояла из комбинации механических и электрических систем. Основной принцип ее работы был в том, что при каждом нажатии на клавиатуру самый правый ротор сдвигается на одну позицию, но при выполнении определённых условиях сдвигались также и другие роторы. Движение роторов приводило к различным криптографическим преобразованиям при каждом следующем нажатии на клавишу клавиатуры. Для расшифровки сообщений, зашифрованных с помощью “Энигмы”, была создана на основании математической теории и методов обратной разработки специальная машина. Взлом принципа шифрования “Энигмы” оказал большое влияние на ход истории в целом и Второй мировой войны в частности.

На протяжении всего времени существования криптографии создатели шифров прилагали все свои усилия для того, чтобы сохранить секреты своих шифров в тайне, а дешифровальщики в свою очередь старались сделать все возможное, чтобы раскрыть эти секреты. Между двумя этими сторонами всегда шло острое противостояние. С приходом криптографии с открытым ключом и политических споров вокруг использования стойкой криптографии наводит на мысли что к сегодняшнему дню в этом противостоянии, несомненно, побеждают криптографы.

Очевидно, что со временем и уровнем развития технологий способы защиты информации меняются. Большим толчком к этому послужило появление компьютеров. Удобство в использовании и многозадачность этого вида техники привело к тому, что большая часть людей и предприятий предпочитают хранить свою информацию в электронном виде, вследствие чего возникла потребность в защите этой информации.

На сегодняшний день информация может не только помочь, но и навредить. Повсеместное использование локальных компьютерных сетей и объединение их в глобальные сети увеличивает возможности их несанкционированного использования. Все страны мира каждый день сталкиваются с постоянным потоком “компьютерных” преступлений, что требует привлекать больше внимания и сил для организации борьбы с этим видом преступлений. Основываясь на отчетах и прогнозах международной компании “Group-IB”, специализирующейся на предотвращении кибератак можно сделать вывод о том, что существенный размах компьютерные преступления получили в автоматизированных банковских системах.

Повсеместная интеграция компьютеров увеличивает объем хранимой в электронном виде информации. С появлением локальных и глобальных сетей даже отсутствие непосредственного физического доступа к компьютеру не гарантирует сохранность хранящихся на нем ресурсов. Это влечет за собой появление все большего количества специализированных средств защиты информации, которые, как правило, ориентированы на решение только одной задачи обеспечения безопасности системы. Так, организациям, чтобы обеспечить защиту от "компьютерных" преступлений приходится реализовывать большой набор мер. Этот набор в Российской Федерации устанавливают Государственные органы на основании Федеральных законов и подзаконных нормативных правовых актов.

Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 20.03.2021) является одним из центральных документов сферы информационной безопасности в связи с тем, что он регулирует отношения, возникающие:

1. При осуществлении права на поиск, получение, передачу, производство и распространение информации;
2. При применении информационных технологий;
3. При обеспечении защиты информации.

В свою очередь Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ регулируют отношения, связанные с обработкой персональных данных, осуществляемой всеми федеральными органами государственной власти, органами местного самоуправления, юридическими и физическими лицами с использованием средств автоматизации.

Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак, определяет основные понятия, связанные со сферой деятельности этого закона.

Из всего вышеперечисленного можно понять, что вся сфера информационной безопасности юридически регулируется и требует постоянных изменений в связи с изменениями и появлением новых механизмов и средств совершения преступлений в сфере информационных технологий.

Каждый сбой или отклонение в работе компьютерной сети это не только "моральный" ущерб для работников предприятия и сетевых администраторов, но и угроза прекращения функционирования целых сегментов банковских систем, что может привести к ощутимым материальным потерям.

Для уменьшения ущерба нужно грамотно выбирать меры и средства обеспечения защиты информации от кражи, умышленного разрушения, несанкционированного доступа, порчи, чтения и копирования.

Перехваченное сообщение о сбое или отклонении в работе системы может быть использовано злоумышленниками с целью нанесения вреда предприятию или получению собственной выгоды.

Актуальность темы моей выпускной квалификационной работы обусловлена необходимостью защитить информацию об инцидентах, передаваемую в рамках рабочего процесса в сети "Интернет", ввиду важности быстроты реакции на нее, по каналам связи с повышенным риском из-за возможности ее перехвата. Иногда возникает ситуация, при которой передаваемая информация не относится ни к одному из типов информации, которые регулируют нормативные документы. Однако использование этой информации лицами, для которых она не предназначена, может повлечь за собой как репутационные, так и потенциальные финансовые риски. Так, предположим, в банковской системе передается информация о произошедших инцидентах. Пример типового сообщения:

Zabbix ЗиС

Инцидент по проблеме: Проверка потока заявок от RBS

Вам необходимо войти в экстренную ТКС АС ЕФС. Ваше присутствие необходимо для оперативного решения инцидента.

Инцидент создан автоматически 06:03:37 от 2021.04.04

Критичность: Disaster

Код: efs7\_cbp\_0202

В этом сообщение не передается информация, которая могла бы относиться к коммерческой тайне (на основании [Федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне"](http://www.consultant.ru/document/cons_doc_LAW_48699/)) или секретам производства (ГК РФ Статья 1465), или какому-либо другому виду информации, подлежащему защите.

КОНЕЦ

Рассмотрим пример ситуации. В системе произошел критический инцидент: перестали вычитываться заявки на получения кредитов. Исправление, которое необходимо внести требует согласование с начальником отдела сопровождения. Из-за того, что важная информация не может быть передана безопасно на личный телефон, приходится использовать рабочий или домашний компьютер, на котором организовано удаленное подключение. Доступ к этим устройствам начальник имеет далеко не всегда. Допустим, он отошел в магазин, за это время произошел инцидент, о котором начальник узнает только когда вернется из магазина и получит доступ к компьютеру, за это время может произойти влияние на клиента (наберется критическая масса нерассмотренных заявок), что повлечет репутационный и потенциальный финансовый ущерб для всего банка.

Основной целью выпускной квалификационной работы является нахождение оптимального варианта решения проблемы: передача важной информации в общедоступной сети.

Достижения указанной цели требует решить ряд определенных задач.

Во-первых, проанализировать возможные варианты решения основной цели, во-вторых, исследовать и проанализировать методы и средства защиты информации, и, в-третьих, рассмотреть задачи защиты информации в отдельной корпоративной сети (на примере Публичного акционерного общества "Сбербанк России"). В качестве отправной точки для исследования поставленных задач мною использовались материалы общедоступных публикаций сети "Интернет".

При написании второй главы мною была использована работа, написанная во время прохождения практики в ПАО “Сбербанк”.