УНИВЕРСИТЕТ ИТМО

А.А. Воробьева, И.С. Пантюхин

ИСТОРИЯ РАЗВИТИЯ ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Санкт-Петербург
2017

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

УНИВЕРСИТЕТ ИТМО

А.А. Воробьева, И.С. Пантюхин

История развития программно-аппаратных средств защиты информации

Учебное пособие

УНИВЕРСИТЕТ ИТМО

Санкт-Петербург

2017

Воробьева А.А., Пантюхин И.С. История развития программно–аппаратных средств защиты информации.– СПб: Университет ИТМО, 2017. – 62 с.

Учебное пособие разработано для методической помощи бакалаврам, обучающимся по направлению подготовки 10.03.01 «Информационная безопасность».

В учебном пособии рассмотрены вопросы развития средств обеспечения компьютерной безопасности с момента появления первых компьютеров в 1950–х годах. Приводится не только хронология возникновения определенных средств защиты, но также сделана попытка дать характеристику каждого этапа, описать эволюцию угроз информационной безопасности, обозначить события, приведшие к возникновению новых средств защиты информации.

Учебное пособие может быть рекомендовано бакалаврам, осуществляющих подготовку по направлению «Информационная безопасность», руководителям и специалистам информационных, юридических и кадровых служб, IT подразделений и подразделений по технической защите информации.

Рекомендовано к печати Ученым советом факультета ИБКТ, 18 января 2017 г., протокол No1.

Университет ИТМО – ведущий вуз России в области информационных и фотонных технологий, один из немногих российских вузов, получивших в 2009 году статус национального исследовательского университета. С 2013 года Университет ИТМО – участник программы повышения конкурентоспособности российских университетов среди ведущих мировых научно–образовательных центров, известной как проект «5 в 100». Цель Университета ИТМО – становление исследовательского университета мирового уровня, предпринимательского по типу, ориентированного на интернационализацию всех направлений деятельности.

Оглавление

Введение.....5
Краткая предыстория.....7
I этап. 1950 – середина 1970–х. Мейнфреймы.....8
Компьютерные преступления. Первые компьютерные преступления, фрикеры и хакеры..... 8
Хакеры.....8
Уязвимости, ARPANET и первые компьютерные вирусы.....9
Компьютерные преступления.....11
Защита информации в период 1950-х – середины 1970–х годов..... 14
Военные и правительственные организации. Первое осознание проблемы компьютерной безопасности.....14
Начало развития компьютерной безопасности.....15
Криптография.....16
Системы разграничения доступа.....16
Системы контроля управления доступом.....18
II этап: вторая половина 1970–х – начало 1990–х годов. Персональные компьютеры и сети.....20
Компьютерные преступления. Хакеры – компьютерные преступники..... 21
Компьютерные взломы.....21
Компьютерные вирусы и эпидемии.....23
Защита информации в период второй половины 1970–х – начала 1990–х годов..... 26
Коммерческие организации, персональные компьютеры и сети....26
Системы разграничения доступа.....28
Межсетевые экраны.....30
Криптография.....31
Антивирусное программное обеспечение.....33
III этап: 1994 – начало 2000–х. World Wide Web и Microsoft.....35
Компьютерные преступления. Расцвет..... 37
Компьютерные вирусы.....37
Компьютерные взломы.....41
Компьютерное мошенничество и угрозы электронной коммерции.....41

Отказ в обслуживании 43
Защита информации в период с 1994 года до начала 2000–х 44
Криптография, новые стандарты и технологии 44
Специализированное ПО 45
Системы разграничения доступа 48
Беспроводная связь, уязвимости и стандарты защиты 50
4 этап: вторая половина 2000–х – настоящее время 52
Новые технологии и угрозы 52
Социальные сети 52
Инсайдеры 53
Индустрия 4.0 и киберфизические системы 54
Каналы реализации угроз и современные программно–аппаратные средства защиты информации 58
Библиография 60

Введение

Практически всегда появление новых методов и технологий защиты информации является ответной реакцией на появление новых видов угроз и проведение атак нового типа. Именно по этой причине развитие защиты информации и информационной безопасности тесно связано с историей хакерства.

Для того чтобы проследить историю развития компьютерных преступлений, необходимо обратиться к истории компьютеров и компьютерных сетей. Появление новых типов компьютерных атак всегда связано с развитием и появлением какой–то новой технологии (объединение компьютеров в сеть, появление персональных компьютеров и Интернета, развитие технологий беспроводной связи). Таким образом, можно выделить четыре основных этапа развития компьютерных и информационных технологий.

Таблица 1. Периодизация развития средств защиты информации.

	Период	Контекст	Виды защиты информации
1	1950–вторая половина 1970–х гг.	Мейнфреймы, фрикеры и первые хакеры.	Меры физической и организационной защиты, средства инженерно–технической защиты.
2	вторая половина 1970–х – начало 1990–х гг.	Персональные компьютеры и сети.	Защита от внешних угроз, первые программные средства и средства сетевой защиты.
3	1994–2000 гг.	World Wide Web и Microsoft. Компьютерные преступления. Расцвет.	Развитие программно–аппаратных средств и средств сетевой защиты.
4	2001–настоящее время	Кибербезопаность. Кибертерроризм, социальные сети и Интернет–вещей. Обострение проблемы инсайдеров.	Программно–аппаратные средства защиты от внутренних угроз, средства обнаружения утечек. Развитие систем прогнозирования и предотвращения атак.

Говоря об истории развития защиты информации, можно сказать, что она прошла два основных крупных этапа:

1. Развитие средств защиты информации по запросу военных и правительственных организаций. Меры защиты разрабатывались в закрытых научных и исследовательских организациях под полным контролем правительства, военных и спецслужб.

2. Развитие средств защиты информации по запросу коммерческих организаций и пользователей. Меры защиты разрабатывались совместно ИТ–компаниями и научными организациями.

Начиная с 1950–х и практически до начала 1990–х, защита информации в основном была задачей военных и правительственных организаций. Появление же всемирной паутины привело к тому, что этот вопрос вышел из–под их контроля, и вопросы защиты стали решаться на множестве уровней. Сегодня ответственность за безопасность лежит на каждом из участников информационных процессов, на каждом пользователе, разработчике, компании.

Краткая предыстория

История современных компьютеров начинается в XIX веке с первых попыток создать программируемое вычислительное устройство Чарльза Бэббиджа, ставшее прообразом современного компьютера. Далее около 1940–х годов появились первые электромеханические машины, которые использовались в Великобритании для взлома кодов Энигмы (Colossus) и применялись в ходе Второй Мировой войны для проектирования самолётов и баллистических ракет (Mark–1 и Z3).

Первые ЭВМ (электронные вычислительные машины), появившиеся практически сразу после окончания Второй Мировой Войны (ENIAC, Манчестерская малая экспериментальная машина, EDVAC и EDSAC), использовались в научных и исследовательских организациях.

I этап. 1950 – середина 1970–х. Мейнфреймы

В 1951 году появились первые коммерческие серийные компьютеры в Европе – Ferranti Mark 1 и в США – UNIVAC–I. К 1960 году в США насчитывалось уже более 5000 ЭВМ, а к 1970 – более 120 000 по всему миру. Такой интенсивный рост и популяризация ЭВМ не могли не привести к появлению т.н. «компьютерных преступлений» в 1960–х годах.

В 1960–1970 годах под компьютерными преступлениями понималось физическое воздействие с целью вывода компьютеров из строя, нелегальное использование компьютерных систем и телефонных линий, компьютерный саботаж.

Доступ к мейнфреймам был физически ограничен и ЭВМ не были объединены в сети, именно поэтому большинство преступлений того времени было осуществлено внутри организации.

Этот этап обладает следующими характерными особенностями:

1. Появление и распространение первых ЭВМ.
2. Появление первых хакеров – лучших компьютерных специалистов.
3. Появление первых компьютерных преступлений: ЭВМ или компьютерная система – цель атаки.
4. Большое число случаев мошенничества с телефонными сетями – фрикинга.
5. Основные угрозы: утечки по техническим каналам, угрозы сбоев в электропитании и угрозы электронного перехвата
6. Появление первых систем и стандартов компьютерной защиты информации.
7. Появление компьютерной криптографии.
8. Появление систем разграничения доступа (СРД) в компьютерных системах, основанных на парольной идентификации.
9. Развитие систем контроля управления доступом (СКУД).

Компьютерные преступления. Первые компьютерные преступления, фрикеры и хакеры

Хакеры

Слово «хакер» появилось в сообществе программистов и системных инженеров Массачусетского Технологического Института (в лаборатории Искусственного Интеллекта и Железнодорожном Клубе Технического Моделирования), где традиционно слово «hack» использовалось для обозначения какого–то нестандартного и «элегантного» технического решения. Позже, в конце 1950–х, слово

утратило исключительно техническую направленность. Это произошло, когда часть исследователей этих групп увлеклась компьютерными технологиями и программированием в стенах компьютерного вычислительного центра: они могли исследовать устройство ЭВМ, писать программы, разрабатывать новые алгоритмы. Именно в это время под словом «hack» стали понимать элегантное и эффективное программное решение, требующее меньшего количества машинных команд и более эффективно управляющее оперативной памятью (в то время крайне ограниченный ресурс). Слово «хакер» в то время носило исключительно положительное значение, отражающее высокую квалификацию.

Несколько позже в университетском вычислительном центре оставили работать только штатных сотрудников, а доступ для студентов был запрещен. Однако они нашли возможность нелегально работать по ночам, когда центр не охранялся. Именно там сформировалось первое хакерское сообщество, объединившее талантливых и увлеченных молодых людей, со своими правилами, философией и этикой. 1950–1960 года многие до сих пор называют «золотым веком хакерства».

Хакеры 1960–х – это талантливые программисты и компьютерные специалисты высокого уровня, способные найти разумное и экстраординарное решение. В основном целью хакеров того времени была попытка более глубоко понять и разобраться, как устроены и как функционируют компьютеры.

Уязвимости, ARPANET и первые компьютерные вирусы

В 1965 году появилась информация о первой уязвимости в ЭВМ. Её обнаружил Вильям Д. Мэтьюс, когда нашел возможность несанкционированного чтения файла с паролями доступа.

В 1969 году в США появилась сеть ARPANET (разработана в агентстве (Advanced Research Projects Agency) Министерства обороны США) – первая глобальная сеть, связавшая крупнейшие научные центры, исследовательские лаборатории и компании, выполняющие оборонный заказ. В последующие несколько лет ARPANET начала быстро расширяться, объединяя все новые и новые центры. Важным для обеспечения безопасности было то, что сеть была основана на идее разделения времени доступа к ресурсам вычислительных центров.

В 1972 году была написана первая программа для отправки и получения текстовых сообщений, которую создатель Рэй Томлинсон назвал e–mail. Программа была доступна только узкому кругу лиц, работающих в вычислительных центрах. Но несмотря на это, появление электронной почты стало новым этапом развития

возможностей общения и связи людей, появилась новая модель взаимодействия пользователей. Помимо e–mail, ARPANET поддерживала удаленное подключение (Telnet) и удаленную загрузку файлов (ftp).

Вместе с тем как ARPANET связала научные центры, она также связала и хакеров. Можно сказать, что сформировалось первое территориально распределенное хакерское объединение, относительно малочисленное, однако, определившее образ хакера периода «до–персональных–компьютеров», когда понятие хакер окончательно утратило свое положительное значение.

Существует мнение, что в начале 1970–х годов в сети ARPANET был зафиксирован первый компьютерный вирус (точнее само перемещающаяся программа) – Creeper, созданный Бобом Томасом для популярной тогда ОС Tenex. Программа получала удаленный доступ по модему, копировала себя в систему, где выводила на экран «I‘M THE CREEPER: CATCH ME IF YOU CAN». Несколько позже появилась вторая программа – Reaper, которая распространялась по сети и при обнаружении Creeper, удаляла его. Автор этой программы неизвестен по сегодняшний день.

1974 год считается годом появления вируса под названием «Rabbit»: он распространялся через носители информации и, попав на машину, самокопировался и занимал системные ресурсы, существенно снижая производительность, что часто приводило к сбоям в работе. Вирус «Rabbit» – первый вирус, вызывающий отказ в обслуживании.

В 1975 году была написана компьютерная игра Pervading Animal, суть которой заключалась в угадывании задуманного игроком животного через наводящие вопросы. Каждый новый вопрос вызывал копирование программы в текущую и все доступные директории, что приводило к переполнению диска. Некоторые эксперты называют игру первой троянской программой.

Компьютерные преступления

Компьютерный саботаж

В основном, преступления, связанные с компьютерами периода 1960–1970–х годов, – это некоторое физическое воздействие на компьютеры с целью их порчи, отключения или уничтожения. Т.к. ЭВМ или мейнфреймы были крайне дорогими, такое воздействие на них было крайне ощутимо для обладателя. Часто этим пользовались злоумышленники, расстреливая, поджигая или взрывая компьютеры. Самым громким и дорогим преступлением того времени можно назвать взрыв в Университете Висконсина, приведший к человеческим жертвам и уничтожению компьютерных данных (ущерб оценивают в 16 млн. долларов США). Самым продолжительным и нелепым был саботаж в Денвере, где в течении двух лет ночной оператор портил считывающие головки жестких дисков, только по той причине, что ему было одиноко, а приезд ремонтной бригады заставлял его чувствовать себя нужным и полезным. Важно, что в этот период хакерство не имело никакого отношения к компьютерным преступлениям.

Подделка компьютерных данных

Одним из старейших видов компьютерных преступлений является подделка компьютерных данных – незаконное или несанкционированное изменение (модификация) информации. Модификация может производиться на всех этапах работы: при вводе или выводе данных, их обработке.

Первое известная подделка компьютерных данных произошла в период 1964–1973 годов в одной из американских финансовых компаний (Equity Funding Corporation of America). В 1964 году, незадолго до опубликования ежегодного финансового отчета, произошел сбой в работе мейнфрема, который сделал невозможным извлечение итоговых расчетов из памяти. Для того, чтобы не задерживать отчет, президент компании распорядился произвести новые компьютерные расчеты, исходя из выдуманного завышенного значения прибыли. Завышение значений прибыли и ввод поддельных данных в компьютеры стали позже для них обычной практикой, позволявшей повысить привлекательность компании для инвесторов. Руководство компании совершало еще ряд мошеннических действий, основанных на своей схеме. Однако преступная деятельность была раскрыта, когда один из недовольных сотрудников компании рассказал о ней властям. Руководство и ряд сотрудников были арестованы и получили тюремные сроки.

Кража компьютерной информации и вымогательство

В 1971 году произошла первая кража компьютерной информации с целью получения выкупа, когда из Bank of America были украдены две магнитные ленты. Только наличие копий, записанных на лентах данных, позволило собственникам проигнорировать угрозы похитителей.

В 1973 году оператор компьютера похитил 22 ленты и получил за них выкуп.

В 1977 году произошел еще один случай кражи магнитных лент и их резервных копий в США. Представители компании обратились в Интерпол, в результате похититель был арестован в Лондоне, полицией Скотланд Ярда.

Телефонные фрикеры

В 1960–1970х годах компьютеры еще не были так распространены, чтобы спровоцировать появление большого числа компьютерных преступлений. Телефонные сети же наоборот уже довольно давно и прочно вошли в повседневную жизнь.

В конце 1950–х годов, телефонный оператор AT&T (в то время, компания–монополист) начал переход на телефонные сети с автоматическим набором номера. В новых сетях использовались сигналы определенных частот для связи между коммутаторами. Все операции в них производились путем отправки на АТС сигнала определенной тональности: соединение с абонентом, переключение на междугороднюю связь, служебные команды. В 1957 году 8–ми летний Джои Энгрессиа случайно просвистел в телефон на определенной частоте, что привело к разрыву соединения. Этот случай вызвал у него серьезный интерес к устройству и принципам работы телефонных сетей. Позже он научился использовать обнаруженную им уязвимость для различных манипуляций с телефонными сетями. В 1968 году он был задержан ФБР во время нелегального бесплатного разговора по междугородней связи.

В 1960–х годах начало появляться достаточно большое число телефонных фрикеров, которые занимались взломом телефонных сетей. Рост числа подобных преступлений был в том числе обусловлен халатностью сотрудников одного из телефонных операторов, опубликовавших в своей статье «Signaling Systems for Control of Telephone Switching» [1] детальную информацию о частотах, используемых для междугородней связи. В 1971 году произошла еще одна утечка – снова была опубликована статья с полным списком частот, используемых для управления телефонной системой. В 1972

году этот список появился в газете «Sunday Times», что привело к существенному скачку в осведомленности телефонных фрикеров.

В 1971 году Джон Дрэйпер («Капитан Кранч»), считающийся «отцом фрикинга», обнаружил, что подарочный свисток из коробки кукурузных хлопьев выдает сигнал определенной частоты, которая использовалась AT&T для осуществления административного доступа к коммутирующим системам. Однако это не было случайностью – Джон Дрэйпер обладал глубокими знаниями в радиоэлектронике и пониманием устройства телефонных аналоговых сетей.

Дрэйпер служит хорошим примером, иллюстрирующим истинную природу хакерства: чтобы взломать какую–то систему, необходимы серьезные знания и понимание того, как система устроена и функционирует.

Фрикеры того времени изготавливали и пользовались специальными устройствами, т.н. "Multi Frequency box" (позже «blue box»), для генерации сигналов различных частот. Blue box – это довольно простые устройства, состоящее из динамика и кнопочной панели. Вместе с этим, они обладали довольно широким диапазоном действий: бесплатные междугородние переговоры, создание конференций, прорыв сигнала «занято», прослушивание разговоров, разрыв чужого соединения, дозвон на недоступные обычному человеку номера и даже контроль над АТС [2]. В 1971 году вышла статья Рона Розенбаума "Secrets of the Little Blue Box", в которой рассказывалось о фрикерах, существующих уязвимостях и устройстве blue box. Статья привела к популяризации фрикерства и росту числа такого рода преступлений.

В этот период развития ИБ хакеров и фрикеров после поимки и задержания часто приглашали работать в крупные компании в качестве специалистов по безопасности, т.к. именно они обладали необходимыми знаниями, и, что более важно, демонстрировали иной, нестандартный взгляд на системы безопасности.

В конце 1970–х годов было произведено достаточно большое число арестов фрикеров, в том числе и известного Джона Дрейпера. Однако большинству из них удалось избежать наказаний в силу существующих недостатков и недоработок в уголовном кодексе.

Фрикинг оставался довольно распространенным явлением вплоть до появления первых персональных компьютеров. Но в начале 1980–х это «увлечение» или этот вид хакерства заменился актуальным сегодня компьютерным взломом. Многие известные хакеры вышли именно из этой среды (Lex Luthor, Cheshire Catalyst, Nightstalker, Dave Starr, Кевин Митник и Кевин Поулсен). Впрочем, считается, что фрикинг оставался самостоятельным явлением до начала 1990–х годов.

Защита информации в период 1950-х – середины 1970–х годов

Военные и правительственные организации. Первое осознание проблемы компьютерной безопасности

В начале 1950-х компьютеры были крайне редким явлением, в основном они использовались в военных или научных организациях. Своеобразными рубежами защиты служили следующие особенности, благодаря которым, не существовало серьезных рисков компьютерной безопасности:

1. доступ к компьютерам был физически ограничен и имелся лишь у узкого круга лиц;
2. для взаимодействия с компьютерами требовались сложные и узкоспециальные знания и навыки;
3. существовали ограничения устройств ввода/вывода и скорость выполнения операций была достаточно низкой.

Под информационной (компьютерной) безопасностью понималась в основном физическая и организационная защита объектов компьютерной инфраструктуры от кражи, порчи, саботажа и угроз природного характера.

Для предотвращения НСД в компьютерные помещения и помещения, где хранились секретные документы использовался контрольно–пропускной режим, различные типы сигнализаций.

В вопросах именно компьютерной безопасности скорее речь шла о физической безопасности носителей информации, что опять же решалось организационными мерами защиты. Второй вопрос компьютерной безопасности – защита от сбоев в электропитании, которые могли привести к потере информации или к выходу оборудования из строя.

Основную опасность составляли утечки по техническим каналам, например, побочное электромагнитное излучение. Угрозу электронного перехвата осознали в 1950–х годах, когда обнаружили, что излучения от мейнфреймов можно перехватить и расшифровать, и восстановить производимые на них операции.

В конце 1950–х был принят первый стандарт TEMPEST (Transient Electromagnetic Pulse Emanation Standard), касающийся допустимого уровня побочного электромагнитного излучения в системах обработки конфиденциальной информации. Меры, принимаемые по стандарту, ограничивались созданием специальных барьеров или оболочек, экранирующих возникающие излучения (пассивные средства защиты). Они могли окружать специальную компьютерную комнату или целое здание, но в основном применялось, как часть компьютерной системы. Также стандарт подразумевал использование генераторов шума и электромагнитных излучений.

В 1960–1970–х годах под безопасностью по–прежнему понималась безопасность данных, содержащихся в хранилищах и базах данных. В это время начали применяться электронные системы контроля управления доступом, появились первые парольные системы разграничения доступа.

Под защитой информации (данных) понимались меры, принимаемые для предотвращения возникновения нежелательных событий, как преднамеренных, так и непреднамеренных, которые могут привести к потере данных.

Примерно в 1960–х годах начинает проявляться интерес к вопросам безопасности со стороны научного сообщества, начинают появляться открытые публикации по компьютерной безопасности. Но только в начале 1970–х начали появляться первые работы, в которых затрагивалась тема безопасности операционных систем (IBM Data Security and Data Processing Manuals Finding Aid).

В силу малого распространения сетей, при обеспечении сетевой безопасности решались исключительно вопросы обеспечения альтернативных маршрутов подключения к сети ARPANET.

Начало развития компьютерной безопасности

Примерно во второй половине 1960 годов с развитием проекта ARPANET появилось осознание опасности потенциальных угроз компьютерной безопасности. Её родоначальником считается Виллис Вейр (Willis Ware). Активные работы по исследованию проблем безопасности он начал в 1960 годах, подчеркивая необходимость защиты компьютеров и компьютерной информации в связи с ростом зависимости от них государства.

Сложившиеся правила организации работы с конфиденциальными документами стали неэффективны с появлением и внедрением подхода разделения рабочего времени в ARPANET. В существующей системе не было возможности разделения данных и предоставления доступа в соответствии с полномочиями. Первые попытки создания систем разграничения доступа относятся именно к этому этапу – середина 1960 годов – и были предприняты совместно Вейром и Бернардом Питерсом.

В 1967 году группой экспертов (научный совет обороны в рамках Министерства обороны США) были представлены выводы о необходимости разработки единых стандартов и протоколов компьютерной безопасности. В группу входили представители различных организаций (производители оборудования и ПО, ряд государственных организаций и спецслужб, работающих над вопросами обеспечения конфиденциальной информации,

обрабатываемой в компьютерных системах, в интересах Министерства обороны США).

В 1970 году они опубликовали отчет, касающийся контроля безопасности в компьютерных системах. Отчет включал базовые принципы обеспечения безопасности конфиденциальной информации: необходимость решения задач защиты на этапе проектирования системы, принципы открытой и закрытой среды, обрабатывание конфиденциальной информации только в закрытой среде.

В 1970–х годах разрабатывались два типа стандартов безопасности:

1. Стандарты исследования, проектирования, создания, тестирования и эксплуатации безопасных компьютерных систем;
2. Государственные криптографические стандарты.

Криптография

Криптография решала задачи аутентификации, верификации и безопасности военной и правительственной коммуникации. К этому периоду относится период т.н. научной криптографии, начавшийся в 1930–е годы, характеризующийся созданием криптосистем со строгим математическим обоснованием криптостойкости. В 1960–е годы ведущие криптографические школы подошли к созданию блочных шифров, реализация которых была возможна только в виде цифровых электронных устройств [3].

Системы разграничения доступа

В начале 1970–х годов проблемы информационной безопасности только начинали прорабатываться, предпринимались первые попытки увязать работу компьютерной системы с существующей системой классификации секретной информации. Однако на практике это порождало ряд трудноразрешимых проблем. Одна из них заключалась в том, что ЭВМ и ОС были устроены настолько сложно для понимания, что операторы или программисты теоретически могли закладывать в них любые недокументированные функции, не рискуя быть обнаруженными. Вторая крупная проблема была в разделении ресурсов одной ЭВМ на работу с разными уровнями секретности, т.е. люди с разными уровнями допуска фактически взаимодействовали с одним физическим хранилищем.

В период 1970–1980 годов, как уже отмечалось неоднократно, основными заказчиками и инициаторами разработок в области защиты компьютерной информации были военные. Информация, которую было необходимо защитить – сведения, относящиеся к государственной тайне. В США, как и практически во всех странах,

существовала сложившаяся система работы с секретными данными. Документу присваивался один из грифов секретности, доступ к которому имели только лица, наделенные полномочиями (имеющие определенный уровень допуска).

Так, в 1972 году в Министерстве обороны США появилась т.н. концепция «ядра безопасности»: система защиты информации должна быть функционально самостоятельной единицей, взаимодействующей с аппаратной частью, а не частью ОС. Первым таким примером является программа HYDRA. Концепция была разработана в группе Джеймса И. Андерсона. Также этой группой была предложена еще одна концепция – диспетчер (монитор) доступа, для обеспечения разграничения авторизованного доступа и запрета чтения данных с более высоким уровнем секретности (мандатный принцип разграничения доступа).

В 1975 году была разработана модель мандатного разграничения доступа – модель Белла–ЛаПадула, которая по праву считается самой значимой моделью того времени.

Авторы модели определили, что ограничения по вышеописанному принципу являются недостаточными для обеспечения безопасности военных систем обработки конфиденциальных данных, проблема возникла вследствие того, что субъекты могли вести запись данных в документы с более низким уровнем конфиденциальности. Модель Белла–ЛаПадула решала эту проблему.

Система представляется как конечный автомат, с двумя типами состояний: безопасные и небезопасные. Под безопасностью понимается такое состояние системы, при котором обеспечивается конфиденциальность информации.

В модели разрешение доступа определяется соотношением уровня допуска субъекта и уровня секретности объекта. Каждому субъекту и объекту присваивается метка конфиденциальности. Причем субъект, которому разрешён доступ только к объектам с более низкой меткой конфиденциальности, не может получить доступ к объекту с более высокой меткой конфиденциальности. Также субъекту запрещается запись информации в объекты с более низким уровнем безопасности. Наборы уровень доступа/уровень секретности описываются с помощью матрицы доступа.

Модель Белла–ЛаПадула расширяла понятие субъекта (включая в него информационные процессы и программы), пытаясь решить потенциальную угрозу троянов (термин появился также в этот период в АНБ).

В 1977 году появилась модель Биба (Kenneth J. Biba), в основе которой также лежит мандатное разграничение доступа, однако в

основе разделения на уровни лежит не конфиденциальность, а целостность информации. Чем выше уровень целостности объекта, тем выше ценность содержащихся в нем сведений, и тем строже должны быть правила доступа к этому объекту. Соответственно, чем выше уровень субъекта, тем более доверенным он является и тем больше полномочий ему предоставляется.

Параллельно с тем, как развивалось прикладное направление защиты информации и создавались модели, предназначенные для решения конкретных задач защиты в военной сфере, появилось научное направление, в котором исследовалась теоретическая возможность обеспечения защиты информации. В этом направлении был создан ряд теоретических или формальных моделей для абстрактного представления политики безопасности, разграничения доступа или информационных потоков в компьютерных системах. В таких моделях все элементы определяются через абстрактные понятия: «субъект», «объект», «операция». Затем для них математически задаются правила, содержащиеся в политике безопасности, условия функционирования и критерии безопасности. На основании такой модели можно производить математическое доказательство безопасности и построение компьютерной системы.

Первая модель такого типа – дискреционная модель Харрисона–Руззо–Ульмана (Harrison–Ruzzo–UIlman), созданная в 1976 году. В данной модели права доступа определяются на основании матрицы доступа, модель позволяет добавлять и удалять субъекты и объекты, изменять права доступа.

Следующая формальная модель – это модель Take Grant (1976), также модель дискреционного управления доступом. В отличие от предыдущей модели, здесь система представляется как конечный ориентированный граф, узлами которого являются объекты и субъекты, а дуги представляют собой операции, значения на дугах задают права доступа.

Еще одна модель, созданная в 1976 году, – это модель безопасности информационных потоков.

Системы контроля управления доступом

Практика применения электронных систем контроля управлением доступа появилась в 1960–х годах на объектах обработки конфиденциальной информации. До этого задачи по защите конфиденциальных данных решались в основном с помощью организационных мер и физического ограничения доступа (установления режима секретности и контрольно–пропускного режима). Основная цель применения электронных систем – более гибкая и простая настройка правил доступа и контроль за персоналом,

т.к. такие системы позволяют сохранять историю активностей. Сначала применялись СКУД с клавиатурами для ввода индивидуального номера (PIN кода). Несколько позже в качестве идентификатора стали применяться магнитные карты, получившие свое нынешнее название «карты доступа».

В конце 1970–х начали использовать бесконтактные карты (proximity карты) и RFID метки.

II этап: вторая половина 1970–х – начало 1990–х годов. Персональные компьютеры и сети

Появление персональных компьютеров и развитие протокола TCP/IP открыло новый этап в развитии компьютерных преступлений. Сообщество хакеров перестало быть закрытым, новые технологии привели к тому, что ряды «научных или профессиональных» хакеров пополнились хакерами–любителями, появились первые специализированные электронные форумы (Bulletin Board Systems, BBS) и хакерские объединения.

Первым домашним или персональным компьютером, получившим достаточно широкое распространение, был Altair 8800, появившийся в 1972 году.

В 1975 году была основана компания Microsoft и появился их первый программный продукт – интерпретатор Altair BASIC, первый язык программирования для первого персонального компьютера.

В 1976 году была основана компания Apple Computer. В 1977 году появился компьютер Apple 2, рассчитанный на массового пользователя, а не только на инженеров. Именно он стал революционным прорывом в развитии персональных компьютеров.

Появление протокола TCP/IP в середине 1970–х, адаптированного для применения в персональных компьютерах, и начало продаж первых относительно недорогих общедоступных модемов создали новые возможности по объединению ПК в локальные сети, которые в свою очередь существенно расширили глобальную сеть ARPANET.

Развитие персональных компьютеров продолжалось стремительными темпами: появлялись новые модели, конкуренция и серийное производство вели к удешевлению ПК. Персональные компьютеры с возможностью выхода в сеть были крайне популярны у «продвинутой» молодежи. Уже к 1984 году глобальная сеть объединила более 1000 узлов, что привело к появлению системы доменных имен.

В 1978 году появились и приобрели популярность первые доски BBS (Bulletin Board Systems –электронная доска объявлений), благодаря которым произошел настоящий переворот в электронной или онлайн коммуникации.

Практически сразу после появления BBS, общение хакеров переместилось в эту новую среду. Появились первые хакерские доски, на которых обменивались новостями и советами, фрикерскими и хакерскими техниками, выкладывали «пиратские» программы, публиковали и продавали номера кредитных карточек и пароли к

компьютерным системам. Доступ к этим доскам был у любого интересующегося энтузиаста, что в результате привело к изменению облика хакера. BBS продолжались активно использоваться вплоть до появления технологии WWW и первых веб–сайтов.

В 1979 году появился первый коммерческий сервис электронной почты – CompuServe.

В 1983 году ARPANET полностью перешла на использование протокола TCP/IP, что послужило точкой отсчета для начала трансформации ARPANET в Интернет. Без наличия единого стандарта связи распространение сетей попросту было невозможно. В течение 1980–х глобальные сети прочно вошли в жизнь пользователей по всему миру, уже в 1987 году в сети насчитывалось более 10000 хостов по всему миру.

Интернет стал доступен практически всем пользователям по всему миру, появилось новое пространство, не имеющее границ. Также изменился и характер компьютерных преступлений, постепенно он приобретал свои современные черты: удаленность и кроссграничность.

Негативное отношение к хакерам и хакерской деятельности начало формироваться еще конце 1970–х годов. В СМИ хакерами стали называть злоумышленников, осуществляющих несанкционированный доступ к компьютерам.

Компьютерные преступления. Хакеры – компьютерные преступники

Компьютерные взломы

В 1981 году был произведен первый арест за совершение исключительно компьютерного преступления. Иан Мерфи (Captain Zap) был арестован за взлом компьютерной сети компании AT&T, произведенный с его домашнего персонального компьютера. Он изменил систему тарифов, поменяв местами дневной и ночной тариф. Мерфи получил наказание за кражу, а не за компьютерное преступление, однако он стал первым хакером, который был осужден.

В 1983 году на широкие экраны вышел фильм «Военные игры», по сценарию которого хакер проникает в компьютерную сеть Пентагона. Фильм закрепил в массовом сознании образ хакера как преступника.

Как ни странно, считается, что этот же фильм послужил толчком в развитии криминального направления хакерства: у энтузиастов проснулся азарт взломать компьютерные системы правительственных ведомств и научных организаций. Так, группой подростков, известной как «414», были взломаны несколько частных сетей, в том числе сети научных лабораторий, банков и больниц. Ими руководил

исключительно «спортивный» интерес, а не желание получить коммерческую выгоду, что вполне соответствует духу и этике хакеров того времени. Подростки были привлечены за незаконное компьютерное проникновение, однако реальных сроков никто не получил. Отсутствие наказания за компьютерные преступления все еще было обычной практикой в силу отсутствия законодательной базы.

В то время компьютерные преступления были настолько редким явлением, что внимания вопросам обеспечения безопасности практически не уделялось. Зачастую даже администраторы компьютерных систем не были осведомлены о потенциальных рисках, существующих угрозах и защитных мерах. Взломы критически важных объектов группой «414» и осознание потенциального ущерба, который эти взломы могли причинить, наконец–то привели к пониманию актуальности и масштаба этой новой проблемы. В результате в США начались работы по созданию законов о компьютерных преступлениях и разработке первых мер защиты.

В конце 1980–х произошел ряд крупных банковских ограблений с использованием компьютерных систем. В 1988 году Арманд Мур ограбил Национальный банк Чикаго с помощью помощников из числа сотрудников банка и похитил около 70 миллионов долларов. Вскоре он был арестован и осужден на 10 лет лишения свободы. Также был ограблен Национальный банк Вестминстера, хакер, взломав компьютерные системы, похитил более 1,5 миллионов долларов.

Благодаря BBS в начале 1980–х по всему миру начали складываться первые хакерские объединения, такие как Legion of Doom, Masters of Desception (США) и Chaos Computer Club (Германия).

В 1984 году начал выходить первый хакерский журнал 2600 и была проведена первая хакерская конференция. Берлин стал первым в мире городом, рискнувшим провести столь новое, ответственное и знаковое мероприятие. Конференция Chaos Communication Congress привлекла внимание всей хакерской общественности и объединила два враждующих лагеря, хакеров и специалистов по безопасности, для достижения одной общей цели – повышении уровня защищенности информации. Организаторы конференции (Chaos Communication Club) попытались донести до всего мира главную идею, что хакерство – не преступление.

В 1987 году прошла первая конференция на американском континенте – SummerCon. Конференция собрала 20 известнейших американских хакеров, в числе которых были: Tuc, Control C, The Leftist, Lex Luthor, Doom Prophet, Ninja NYC, Forest Ranger и другие [4].

Компьютерные вирусы и эпидемии

До распространения Интернета вирусы в основном распространялись через зараженные дискеты, Интернет же открыл для них совершенно новую безграничную среду.

В 1981 году появился первый настоящий компьютерный вирус Elk Cloner, созданный под ОС компьютеров компании Apple (наиболее распространенных в то время). Elk Cloner появился в одной из компьютерных систем техасского университета и распространялся через дискеты (заражение произошло через дискеты с пиратскими копиями компьютерных игр). Этот случай является интересным с той точки зрения, что здесь фигурируют сразу два типа компьютерных преступлений: собственно, само создание вредоносного ПО и нарушение авторских прав на компьютерные игры, которое и привело к распространению вируса (здесь жертвы первого преступления являются исполнителями второго). Также важно, что в этом первом случае проявилась суть вирусов и их создателей – желание заразить как можно большее число компьютеров.

В 1983 году Лен Эйделман впервые употребил термин вирус к самокопирующимся компьютерным программам. Несколько позже Фредерик Коэн впервые дал точное определение термину «компьютерный вирус» и продемонстрировал разработанную им программу. Коэн определил вирус, как программу, которая «заражает» другие программы и модифицирует их, добавляя функционал для создания собственных копий.

В 1984 году Кен Томпсон (ученый, один из создателей языка С и ОС Unix) впервые рассказал о возможности создании бэкдора в команде login одной из версий ОС Unix. Данная возможность реализовывалась через модификацию компилятора С. При сборке ОС модифицированным компилятором, он встраивал бэкдор в команду логин, а при сборке другого компилятора, в него встраивались функции для генерации уязвимостей. В исходном коде компилятора при этом невозможно было обнаружить свидетельств воздействия.

К середине 80–х годов во всем мире широкое распространение получили компьютеры IBM PC под управлением MS–DOS. В результате того, что одна ОС заняла большую часть рынка, вирусы, разработанные для этой ОС, стали также массовыми. Единообразие используемых ОС и отсутствие адекватных механизмов защиты привели к тому, что появились первые вирусные эпидемии.

В 1987 году произошли две первые вирусные эпидемии, вызванные вирусами Brain (первый вирус для IBM PC–совместимых ПК) и Vienna. Изначально вирус Brain был создан для борьбы с пиратским распространением ПО в Пакистане, однако ситуация вышла

из–под контроля. В итоге зараженными оказались более 18 000 компьютеров по всему миру. Brain был первым стелс–вирусом, скрывающим свое присутствие в ОС: при чтении зараженного сектора вирус подменял его на незараженную версию.

В конце 1980–х было известно о достаточно большом числе уязвимостей в ОС UNIX, в особенности в BSD (Berkeley Software Distribution). В ноябре 1988 года появились первые заявления об атаках на компьютерные системы под управлением различных UNIX систем в научных и правительственных организациях (в том числе NASA). Это была эпидемия первого сетевого «червя», инициированная Робертом Моррисом, аспирантом Корнеллского университета. Он запустил в сеть ARPANET червя, который заразил более чем 6000 компьютеров, забил сеть нежелательным трафиком и нанес ущерб в более чем 100 млн. долларов. Червь Морриса использовал известные уязвимости (в сервере sendmail, сервисах finger, rsh/rexec) в сочетании с подбором паролей по словарю. Он скрывал свое присутствие, удаляя свой исполняемый файл и переименовывая свой процесс в sh (командная оболочка UNIX), также каждые 3 минуты червь ветвился.

Целью создания червя была попытка исследовать уязвимости Unix систем. Моррис получил довольно мягкое наказание, что отражает отношение к компьютерным преступлениям в то время – они все еще не воспринимались как реальные преступления. Моррис не стал создателем концепции вируса или червя, он известен тем, что он первым ее реализовал, продемонстрировав феноменальную скорость распространения.

В конце 1980–начале 1990–х вирусная активность начала расти, появился целый ряд новых сетевых червей (Father Christmas, WANK).

Также в эти годы произошло еще несколько достаточно масштабных по тем временам вирусных эпидемий (Lehigh, Stoned, Jerusalem, Cascade (первый зашифрованный вирус), DATACRIME, Ping–Pong, Form, Michelangelo).

Это были файловые (заражают исполняемые файлы .com и .exe, добавляя в них свой вредоносный код) и загрузочные вирусы, которые блокировали запуск ОС, уничтожали приложении при попытке их запуска, снижали производительность ПК и выполняли различные другие опасные действия.

В 1988 году появился первый троян – FLU–SHOT–4, замаскированный под довольно популярный тогда антивирус. Он распространялся через BBS и уничтожал некоторые сектора жестких дисков и дискет. Троян FLU–SHOT–4 интересен тем, что он проявлялся только после того, как программа была запущена. До этого момента фрагменты вредоносного кода было невозможно обнаружить

в исходном коде программы, даже при исследовании его на уровне машинных команд.

В конце 1980–х году появился еще ряд троянов: Scrambler, маскирующийся под драйвер клавиатуры (KEYBGR.COM); 12–Tricks, распространяющийся как программа для тестирования скорости жесткого диска (CORETEST.COM); PC Cyborg или AIDS, распространяющийся через дискеты. AIDS шифровал записи каталога, заполнял весь диск C: и подменял собой командную строку COMMAND.COM. Фактически троян блокировал работу компьютера и требовал произвести оплату за разблокировку.

В этом же году был обнаружен первый многокомпонентный вирус – Ghostball, заражающий как исполняемые файлы, так и загрузочный раздел жесткого диска. Ghostball открыл новое направление развития компьютерных вирусов. В 1991 году появился новый вирус этого типа – Tequila.

В 1989 году появился первый полиморфный вирус 1260 (Chameleon.1260 или V2PX).

Подводя итог к этому этапу, можно сказать, что в этот период появилось и получило развитие большинство типов современных вирусов:

- файловые и загрузочные вирусы;
- вирусы–компаньоны;
- стелс–вирусы;
- сетевые вирусы, черви;
- полиморфные вирусы;
- многокомпонентные вирусы.

Защита информации в период второй половины 1970–х – начала 1990–х годов

Коммерческие организации, персональные компьютеры и сети

1980–е – это период, когда появились первые реальные угрозы хакерства и компьютерных преступлений. Вирусы и хакеры появились как элементы исследовательских проектов в рамках ведущих университетов, персональные компьютеры и сети сделали эти явления популярными и массовыми, создав реальные угрозы государственным и коммерческим организациям.

Практически до конца 1980–х большинство работ по компьютерной безопасности велись только в интересах правительственных и военных ведомств. Однако широкое распространение ИТ и ПК, рост сетей и увеличение числа случаев хакерских атак привело к тому, что проблема безопасности также стала актуальна и для коммерческих организаций. Стандарты и политики, разработанные для военных нужд и работы с конфиденциальными данными, совершенно не подходили для коммерческих организаций.

В 1980–ых годах коммерческие организации только начинали активное внедрение компьютерных технологий в свою деятельность. Вопросы безопасности в основном решались исключительно на уровне парольных систем идентификации/аутентификации, часто не существовало даже простых требований к выбору пароля, а логин (обычно реальное имя пользователя) часто совпадал с паролем.

К концу данного периода компьютерная безопасность уже стала восприниматься как сложное многогранное явление, пришло понимание того, что необходимо предпринимать более комплексные меры защиты. Так компьютерная безопасность стала включать в себя обеспечение конфиденциальности данных и доступности компьютерных ресурсов, защиту процессов от неправомерного использования или несанкционированных изменений. Тем не менее вопросы целостности данных и их несанкционированной модификации по–прежнему стояли на втором плане.

Также к концу 1980–х начали появляться новые методы идентификации и аутентификации, более стойкие по сравнению с парольными системами. Криптография получила широкое распространение в компьютерных сетях коммерческих организаций, открыв новые направления в электронной коммерции.

Однако считается, что даже в конце 1980–х годов вопросы компьютерной безопасности не воспринимались столь остро, и системные администраторы часто не применяли никаких мер защиты, что и привело к появлению такого явления как вирусные эпидемии и расширению хакерского арсенала.

Появление Интернета, повсеместное распространение компьютеров и сетей, развитие клиент–серверных технологий привели к тому, что вопросы обеспечения компьютерной безопасности в 1990–х стали вопросами, требующими безотлагательного и качественного решения для обеспечения существования и развития любой коммерческой организации. В большинстве случаев в коммерческих организациях не существовало единой политики организации и безопасности доступа в Интернет.

Развитие и переход на технологии клиент–сервер требовали от организации обеспечения безопасности на клиентской стороне. В это время особую популярность завоевала технология тонкого клиента, когда все важные операции и «чувствительные» данные вынесены с клиентского ПК на безопасный сервер.

В ответ на возникающие потребности коммерческих организаций в решениях по компьютерной безопасности, начали появляться первые готовые коммерческие решения и инструменты.

Начиная с самого первого этапа при работе с информацией (как государственной, так и коммерческой) применялся принцип необходимого знания – концепция безопасности, ограничивающая допуск к информации и ресурсам обработки информации в объеме, необходимом для выполнения обязанностей заинтересованного уполномоченного лица [5]. Появление Интернета и перенос ряда услуг в онлайн среду во многом затруднило применение этого подхода, т.к. предоставление доступа по умолчанию производилось без прохождения каких–либо процедур идентификации. Необходимо было развитие технологий обеспечения безопасности и разграничения доступа в онлайн приложениях. Результатом стало развитие прикладной криптографии, применяемой для обеспечения конфиденциальности и целостности данных, передаваемых по сетям, технологий обмена ключевой информацией и появление различных межсетевых экранов.

Самой опасной угрозой стали компьютерные вирусы.

Присоединение корпоративных сетей к Интернету привело к возникновению ряда угроз:

1. вызванных, уязвимостями различных сетевых протоколов (в частности, TCP/IP) и систем;
2. атаки вирусов и сетевых червей;
3. опасность осуществления НСД к данным или ресурсам компьютерной системы;
4. несанкционированный перехват данных и их модификация;
5. кража паролей.

В качестве основных источников угроз и инициаторов атак выступали хакеры, конкурирующие организации, инсайдеры (в том числе недовольные сотрудники).

Стремительный рост опасности указанных угроз и числа инцидентов безопасности привели к необходимости развития механизмов разграничения доступа, идентификации/аутентификации, обеспечения конфиденциальности и целостности данных.

Системы разграничения доступа

Модели разграничения доступа для коммерческих организаций

В 1987 году появилась первая публикация по теории разграничения доступа в коммерческих компьютерных системах, авторами публикации были David D. Clark и David R. Wilson. Модель Кларка–Вилсона отходила от привычной и принятой у военных концепции уровней доступа и была построена с учетом тенденции внедрения ПК во все сферы деятельности коммерческих организаций.

В отличие от целей защиты информации в военной области (обеспечение конфиденциальности), основной целью в коммерческих организациях является защита целостности. Под этим подразумевается защита информации от несанкционированной модификации, в том числе в следствие компьютерного мошенничества и ошибок. В отличие от модели Белла–ЛаПадула (множество субъектов–множество объектов), в модели Кларка–Вилсона компьютерная система рассматривается как система со множеством приложений.

Операциями доступа в модели являются программы, выполняющие множество различных действий (транзакции), а не простые операции чтения–записи, как, например, в предшествующих моделях.

Основная идея обеспечения целостности заключается в том, что в системе разрешены только «корректные транзакции» и обеспечено «разделение обязанностей», т.е. модифицировать данные может только определенный набор программ. Программы являются дополнительным уровнем в модели между данными и пользователями. Субъекты могут выполнять только программы из определенного набора, а доступ к определенным данным есть только у определенных программ. Непосредственный доступ к данным для пользователей невозможен. В модели впервые сама система безопасности рассматривается как такая же программа и ее защищенность также оценивается.

Кроме того, модель решала проблему подмены пользователя в момент между идентификацией и выполнением операции, т.к. производилась дополнительная верификация субъекта до и после

выполнения операции. Модель Кларка–Вилсона, с точки зрения обеспечения целостности, считается одной из самых совершенных.

В 1989 в Великобритании появилась модель компьютерной безопасности «Китайская стена». Своим появлением она обязана Биржевому краху 1929 года, с которого в США началась Великая депрессия. В ответ на это событие была введена политика о конфликте интересов или политика «китайских стен» для регулирования деятельности брокерско–дилерских компаний. Китайская стена должна была разделять потоки данных возникающие, в результате разных видов деятельности компании. В частности, информация, полученная в рамках одной сферы деятельности компании, не должна оказывать влияние на принятие решений в другой сфере деятельности, для которой она является конфиденциальной [6]. Т.е. Китайская стена разделяет потоки конфиденциальной информации внутри одной компании.

К 1986 году компьютеры плотно вошли в повседневную деятельность финансовых компаний, но политика Китайской стены должна была соблюдаться также и для информации, циркулирующей в компьютерных системах. Применительно к информационным системам Китайская стена должна была защищать от возникновения конфликта интересов, внутреннего мошенничества, инсайдерской торговле и прочих внутренних угроз. Она реализовывала набор правил доступа, которые могли меняться автоматически и динамически после того, как субъект обращался к некоторой информации (далее доступ на определенные операции, вызывающие конфликт интересов, для него закрывался).

В 1982 году появилась новая формальная модель Гогена–Мезигера (Goguen–Meseguer), открыв новый тип моделей – моделей информационного невмешательства.

Биометрические системы разграничения доступа

Вообще биометрия и биометрическая идентификация имеет долгую историю. Считается, что отпечатки палацев и некоторые другие физиологические и физиогномические особенности использовались для идентификации и установления личности в древнем Китае и древнем Египте. Отпечатки пальцев стали впервые использоваться для идентификации преступников в XVIII веке.

Первые полуавтоматические системы распознавания лиц появились в 1960–х годах. Тогда же были начаты активные исследования по автоматизации распознавания и идентификации по другим биометрическим характеристикам (отпечатки пальцев, голос, подпись).

В 1969 году ФБР внедрила первую автоматическую систему идентификации по отпечаткам.

В 1974 появились первые коммерческие системы биометрической идентификации по геометрии руки.

В течение 1970–1980–х годов продолжались исследования, направленные на совершенствование систем биометрической идентификации: создание сканеров, алгоритмов сравнения, поиск лучших признаков. Были созданы первые системы идентификации по голосу человека. В это же время была доказана возможность идентификации по сетчатке глаза, были получены первые результаты и патенты, и вскоре был обнаружен достаточно эффективный алгоритм идентификации (Dr. John Daugman), на него также был получен патент (владелец компания Iridian Technologies). Сегодня эта разработка и патент лежат в основе всех коммерческих разработок по распознаванию сетчатки глаза.

В 1991 году появилась первая система распознавания лиц в реальном времени.

Начав свое активное развитие в 1980–х, системы биометрической идентификации продолжали совершенствоваться, повышалась точность распознавания. Системы были достаточно дороги и в основном применялись правительственными и военными организациями, а также крупными коммерческими компаниями. Основными целями применения биометрии правоохранительными органами была идентификация личности (поиск преступников и опасных лиц (в аэропортах, на спортивных мероприятиях)). В коммерческих организация системы применялись в СКУД для физического разграничения доступа, контроля рабочего времени и идентификации сотрудников.

Начиная с 1990–х годов, технологии биометрической идентификации расширялись, снижение стоимости оборудования и снижения ложных срабатываний привели к повышению спроса на эти технологии.

Биометрические сканеры стали применяться для обеспечения доступа к ПК. Позже, в начале 2000–х годов, развитие технологий биометрической идентификации позволило внедрить ее в переносные устройства. Так, в 2004 году в ноутбуках впервые появились сканеры отпечатков, а в смартфонах – в 2013 (Apple iPhone).

Межсетевые экраны

В 1988 году появлялись первые открытые публикации по технологиям межсетевого экранирования и пакетной фильтрации.

В начале 1990–х появились первые коммерческие межсетевые экраны (брандмауэры, файерволлы), позволяющие разграничить глобальные и частные сети. Вообще, сама технология и первые устройства были разработаны в компании Cisco в 1980–х годах.

Развитие технологий межсетевого экранирования происходило по восходящей в модели OSI: сначала появились фильтры на сетевом и транспортном уровне, позже – на сеансовом уровне и уровне приложений.

В основе работы межсетевых экранов, созданных на этом этапе, лежит концепция, что все легальные пользователи находятся внутри сети, а все нелегальные – вне ее.

Первыми файерволлами были простые фильтрующие маршрутизаторы, которые позволяли фильтровать трафик по заранее заданным правилам, по различным полям заголовка пакетов (например, IP адрес отправителя или получателя, номер порта). Такие файерволлы позволяли фильтровать трафик только на сетевом и транспортном уровнях, но не на уровне приложений или конкретных пользователей. Среди первых компаний разработчиков можно выделить Cisco, 3COM и Wellfleet [7].

Следующим этапом развития межсетевых экранов было появление в 1989–1990 годах шлюзов сеансового уровня.

В период 1991–1994 года наиболее популярными были межсетевые экраны Raptor Systems Eagle, Advanced Networks and Services' (ANSi inter–Lock, Trusted Information System's (TIS) Gauntlet и Checkpoint Software's Firewall [8].

Криптография

Развитие вычислительных средств и повышение их производительности в 1970–х, позволило создать криптографические системы с более высокой криптостойкостью, чем все существующие на тот момент. В этот период появилась компьютерная криптография [3].

В конце 1970–х годов у коммерческих организаций возникла острая необходимость встроить шифрование в только что появившуюся новую технологию – электронную почту, в основном запрос был сформирован нефтяными и банковскими компаниями.

В этот период шифрования частных коммуникаций не существовало, прослушивание частных переговоров было простой задачей для правительственных структур, таких как АНБ. Шифрование было доступно только для военных или правительственных организаций, а обмен ключами производился только через один из государственных центров управления ключами.

В 1980–е годы правительством США (в частности АНБ) предпринималось большое количество попыток ограничить развитие криптографии путем введения запретов на исследования в этой области и запретов на ее использование для частных нужд. АНБ старалось сохранить за собой право и возможность контролировать типы и качество шифрования, применяемого частными лицами и организациями, как на территории США, так и за рубежом. Коммерческие организации осознавали, что стандарты шифрования, разрабатываемые в АНБ не являются криптостойкими и потенциально могут содержать закладки.

Именно этот факт послужил причиной создания Уитфилдом Диффи и Мартином Хеллманом ассиметричных шифров и систем с открытым ключом (1975 год). Диффи, работая в одной из компаний подрядчиком МО США, заинтересовался вопросами повышения безопасности компьютерных вычислений и возможностью применения математических и криптографических методов в частных коммуникациях.

Открытие Диффи и Хеллмана сделало криптографию доступной обычным людям и позволило применять ее для защиты частной информации. Для широкого практического применения криптографии необходимо было решить проблему обмена ключами без участия центра и без обмена самим секретным ключом. Проблема порождала две сложные задачи: обеспечение целостности и аутентичности информации – надежное шифрование и подтверждение подлинности отправителя. Однако алгоритм Диффи–Хеллмана не мог решить задачу аутентификации сторон.

В 1978 была опубликована работа, содержащая описание новой криптосистемы RSA (Великобритания, авторы Рон Ривест, Ади Шамир и Леонард Адлеман), в которой решалась проблема взаимной идентификации.

Алгоритм RSA обеспечивал необходимую стойкость и надежность. В 1982 году была основана компания RSA Data Security, которая в том числе занималась выдачей лицензий на использование алгоритма RSA в программных продуктах других фирм. В частности, он был встроен в продукты Microsoft, Apple и в IBM Lotus Notes.

В 1989 году начинается применение алгоритма в Интернет для шифрования, а несколько позже для цифровой подписи.

Ассиметричная криптография, помимо того, что позволила решить свою первую прикладную задачу – шифрование частных коммуникаций (электронной почты), открыла несколько перспективных направлений применения – системы электронной цифровой подписи и электронной коммерции.

Антивирусное программное обеспечение

С появлением первых вирусов стали разрабатываться первые программы антивирусы. Как уже говорилось выше, первый из них появился в 1971 году – программа Reaper (жнец) для удаления вируса Creeper (лиана).

До того, как Интернет приобрел повсеместное распространение, вирусы в основном распространялись через дискеты. Антивирусное ПО этого периода в основном должно было проверять исполняемые файлы, загрузочные секторы дискет и жестких дисков.

Существует мнение, что первые специализированные антивирусные программы появились в 1984 году: CHK4BOMB и BOMBSQAD. Они основывались на синтаксическом анализе и позволяли анализировать тексты файлов ОС для выявления участков подозрительного кода и предотвращать операции, выполняемые вредоносными приложениями через BIOS.

Помимо антивирусов существовали своеобразные вирусные базы, распространяющиеся через BBS и представлявшие из себя текстовые файлы со списком опасных программ, которые пользователи загружали в файлообменники. Например, файл «The Dirty Dosen – An Unloaded Program Alert List»: в первоначальный список входили 12 вредоносных программ, с появлением новых вирусов список пополнялся. Быстрый рост числа вирусов продемонстрировал, что данный подход является недостаточным и необходимо создание других мер по защите – антивирусного ПО.

В результате, в 1985 году появился первый резидентный антивирус DRPROTECT, работающий в фоновом режиме и производящий сканирование операций, выполняемых с файлами. Программа блокировала все операции, выполняемые через BIOS, и в случае обнаружения операции требовала перезагрузки системы.

В 1987 году появились первые антивирусы с эвристическим анализом программного кода – Flushot Plus (Ross Greenberg) и Anti4us (Erwin Lanting).

В 1988 году появился первый антивирус McAfee Virus Scan (создатель John McAfee). В 1989 году была основана компания McAfee, которая в течение двух последующих лет была единственной компанией, специализирующейся на разработке антивирусов. А в 1991 году появился антивирус от крупной компьютерной компании Symantec – Norton AntiVirus.

Сигнатурный анализ (поиск характерных фрагментов кода в файловой системе) появился в 1988 году в первой российской антивирусной программе Aidstest (Лозинский Д.Н.). В 1989 году

компания IBM выпустила антивирус VIRSCAN, в котором также использовался поиск по сигнатурам.

К концу этапа насчитывается уже несколько тысяч известных вирусов. Антивирусные компании ведут активные разработки, в том числе по борьбе с полиморфными вирусами, появляется ряд достаточно эффективных решений.

В 1990 году в Германии был создан Европейский Институт Компьютерных Антивирусных Исследований (European Institute for Computer Anti–virus Research), сегодня – это одна из крупнейших и наиболее значимых международных организаций, объединяющей практически все крупные антивирусные компании [9].

В 1992 году в «Лаборатории Касперского» был разработан первый антивирус, основанный на эвристическом анализе и позволяющий бороться с ранее неизвестными вирусами.

III этап: 1994 – начало 2000–х. World Wide Web и Microsoft

Настоящий переворот в использовании Интернета произошел в результате появления новой технологии WWW (World Wide Web). В 1991 году Тим Бернерс–Ли создал первые веб–страницы, положив начало новой технологии www, также им были созданы URI, URL, HTTP, HTML. До этого Интернет служил для передачи файлов, отправки электронной почты и ряда других сервисов. Веб–страницы полностью изменили возможности коммуникации и получения информации, каждый пользователь из любой точки мира мог обратиться по некоторому адресу и получить информацию, просмотреть фотографии и изображения. Интернет стал доступным и зрелищным, это была новая концепция доступа – «все для всех». Вместе с тем, как Интернет стал новой средой и новым пространством (наряду с воздушным, морским и космическим), возникли новые угрозы и произошел резкий скачкообразный рост компьютерных или киберпреступлений.

В 1994 году вышел первый полнофункциональный веб–браузер – Netscape Navigator. Именно с него началось повсеместное использование Интернета как «набора» веб–сайтов. Естественно, что хакеры также быстро освоили новое пространство, произошел переход с BBS на новые специализированные веб–сайты.

На хакерских сайтах, также как на BBS, продолжала размещаться информация о способах взлома и уязвимостях, публиковалось содержимое взломанных баз данных (в том числе учетных записей), размещались различные хакерские утилиты. Однако существовало одно важное и ключевое отличие – эти сайты были доступны всем желающим. Именно в 1990–е начинает появляться большое количество готовых хакерских программ, не требующих от злоумышленника каких–либо технических знаний и навыков. А благодаря распространению Интернета и доступности ПК эти программы нашли своего массового потребителя. Примерами таких программ могут служить программы для подбора паролей, взлома сетей, реализации атак на отказ в обслуживании: winnuke, Netbus и BackOrifice (возможность несанкционированного удаленного доступа к ПК под Windows 95 и 98). В 1999 году появился первый сканер уязвимостей sscan.

Также ярким примером выступает программа, нацеленная на атаку одной конкретной компании AOL – AOLHell, которую мог скачать любой желающий. В результате их чаты и почтовые ящики были полностью заполнены спамом, который практически парализовал работу компании.

Считается, что 1990–е – это период массового безнаказанного хакерства, в первую очередь обусловленного отсутствием и несовершенством механизмов безопасности, наличием огромного числа уязвимостей в ОС (Windows и UNIX), а также возможностью получить доступ к компьютерным системам, благодаря подключению их к Интернету и массовым использованием одинакового ПО и ОС (Windows и Unix–подобных систем).

В середине 1990–х хакерское сообщество стало меняться, приобретая все большую численность и окончательно закрепив за собой криминальный характер. Появление большого количества фильмов о хакерах, в некоторой степени романтизирующих образ хакера, привело к росту популярности этой темы среди молодежи. Эти же фильмы обозначили проблему безопасности и, в частности, опасность вирусов для масс, что также привело к повсеместному распространению антивирусов.

В 1993 году прошла первая конференция DefCon. Она сразу же выделилась своей массовостью и разнообразностью тематик. Сегодня это крупнейший съезд хакеров, объединяющий не только тех, кто взламывает сети, но и тех, кто их защищает и поддерживает. DefCon привлекает огромное внимание мировой общественности и является одним из ключевых мероприятий в области защиты информации.

В 1995 году вышла ОС Windows 95, в основном предназначенная для использования в домашних ПК и не требующая от пользователей практически никаких специальных навыков для работы. В Windows 95 старые вирусы, написанные под MS–DOS, не работали, и какое–то время ОС была достаточно безопасной относительно вирусной угрозы. В 1999 году появилась Windows 98 со встроенным браузером Internet Explorer и Outlook. В сегменте серверных ОС Microsoft с Windows NT также заняла огромную нишу.

В новых ОС было выявлено большое число серьезных уязвимостей, т.к. технологии безопасной разработки были недостаточно развиты и вопросы безопасности по–прежнему считались второстепенными. В 1998 году компьютеры НАСА и Министерства Обороны США подверглись DoS атаке, использующей уязвимости ОС Microsoft NT и 95.

Так, 1999 год – это год исключительной хакерской активности, вызванной исследованием уязвимостей Windows 98 и других продуктов Microsoft. Регулярно публиковалась информация о новых ошибках и уязвимостях, разработчики реагировали выпуском обновлений для их устранения.

Можно сказать, что частично именно благодаря ошибкам в ОС от Microsoft появилось такое обширное количество инструментов для защиты ПК от различных производителей.

В конце 1990–х хакерство выходит на коммерческую основу, новые уязвимости перестают открыто публиковаться для всех желающих, а продаются или эксплуатируются самостоятельно людьми, которые их обнаружили. В это время активно начинает развиваться промышленный и экономический шпионаж с использованием компьютерных систем, а также компьютерные атаки на конкурирующие компании. Примером такой борьбы может служить случай взлома сайта компании регистратора доменных имен InterNIC (взломан основателем компании AlterNIC – Eugene Kashpureff).

Часто действия хакеров данного периода, как и современных хакеров, связаны с вымогательством путем угроз разглашения информации, угроз DDoS атаками и пр.

Компьютерные преступления. Расцвет

Компьютерные вирусы

К началу периода существовало огромное число самых разнообразных вирусов, и уже произошло несколько обширных вирусных эпидемий, которые принесли многомилионный ущерб. Вирусные технологии на данном этапе продолжают развиваться, создаются новые сложные вирусы. Несмотря на то, что проблема вирусов существовала уже относительно давно, во множестве стран создание вирусов законодательно не преследовалось.

Вирусы в различных ОС

В 1996 году появился первый вирус под Windows 95 – Win95.Boza, и первый же резидентный вирус Win95.Punch. Первая вирусная эпидемия среди ПК под управлением Windows произошла также в этом году и была вызвана вирусом Win.Tentacle. Это было только начало лавинообразного роста числа вирусов под ОС от Microsoft.

В 1998 году появились первые полиморфные вирусы – Win95.HPS и Win95.Marburg. В этом же году случилась одна из самых разрушительных эпидемий, вызванная вирусом Win95.CIH или Чернобыль.

К концу 1990–х стало очевидно, что основной целью хакеров является ПО и ОС от Microsoft, а политика выпуска обновлений на обнаруживаемые уязвимости была неэффективной. Ответной мерой стало принятие в начале 2000–х новой политики безопасной разработки в компании Microsoft – Trustworthy computing Security Development Lifecycle (SDL). Принятие новой политики позволило существенно снизить количество уязвимостей, так количество уведомлений по технической безопасности (бюллетеней безопасности),

публикуемых Microsoft Security Response Center, в Windows 2000 до принятия SDL – 62, а в Windows Server 2003 (с применением SDL) – 24 [10].

После этого существенного качественного скачка в обеспечении безопасности, активность хакеров в основном сместилась в сторону создания средств массовой рассылки и почтовых ботов, работающих в обход файерволлов через веб–браузеры и позволяющих производить рассылку спама, вредоносного ПО и распределенные атаки на отказ в обслуживании [11].

В начале 2000–х появилось несколько довольно опасных сетевых червей, массовость заражения которыми вызвана единообразием используемых ОС. Это черви Code Red и Blaster, многовекторные черви – Nimda (2001) и Fizzer (2003), Slammer (самый быстро распространяющийся червь, 2003). Они использовали уязвимости в ОС Windows (95, 98, NT, 2000, XP) и серверах Microsoft (IIS, Server 2003, SQL Server и пр.). Все эти черви также привели к эпидемиям и многомиллионным убыткам.

Часто новые вирусы разрабатывались после того, как выходило очередное обновление безопасности от производителя, закрывающее определенный эксплоит. Обновление ПО и ОС выполнялось по желанию пользователей, которые не спешили устанавливать обновления, и вирус легко распространялся от одного не обновлённого ПК к другому. Однако иногда появление вирусов и червей происходило по обратному сценарию – сначала появлялся вирус, потом выходило обновление.

Сетевые черви имели обширное распространение и составляли один из наиболее опасных видов угроз. От них существовал единственный способ защиты – установка патчей от производителей, закрывающих используемые ими уязвимости. Использование межсетевых экранов и антивирусов еще не было столь распространено среди обычных пользователей и в мелких компаниях. Ситуация массовых заражений изменилась только в 2004 году, когда вышел второй пакет обновлений для Windows XP, включающий Брандмауэр Windows – встроенный межсетевой экран.

В этот период получили обширное распространение трояны кейлоггеры, перехватывающие ввод с клавиатуры, и часто использующиеся в промышленном шпионаже. К 2000 году насчитывалось уже более 300 известных кейлоггеров, а к 2004 их число достигло 3753 [12].

В течение 1990–х и начале 2000–х не было зафиксировано ни одной вирусной эпидемии, и сегодня ОС Linux и другие Unix системы считаются самыми защищенными ОС, несмотря на то, что первые

вирусы под FreeBSD и Linux (вирус Snoopy и Bliss) появились еще в 1995-1996 годах.

В 1990–х годах и в других достаточно популярных ОС, таких как OS/2 (разработка IBM) и Mac OS проблема вирусов практически полностью отсутствовала.

Вирусы, использующие уязвимости в популярных приложениях

Стремясь поразить максимальное число компьютеров, хакеры старались разрабатывать вирусы, использующие уязвимости в самых популярных технологиях и приложениях (Java, Corel и пр.).

В 1997 году появился первый сетевой червь, распространяющийся через FTP (File Transfer Protocol).

К 1998 году Интернет–браузеры стали самым коротким путем проникновения на персональный компьютер, разрабатывались новые способы взлома использующие методы социальной инженерии (ссылки на сайты с вредоносным контентом) и технологии создания активного содержимого веб–страниц, способного производить определенные, необходимые злоумышленнику действия.

В 1998 году появились первые скриптовые вирусы, написанные на скриптовых языках (VBScript, JavaScript) и размещаемые в коде веб–страниц. Тогда же появились первые кроссплатформенные вирусы, использующие Java уязвимости.

Макровирусы

Наиболее примечательным событием этого этапа стало создание вируса Concept в 1995 году, положившего начало новому типу вирусов – макровирусов. Макровирусы написаны на макроязыках, встроенных в ряд приложений, например, на Visual Basic.

Вирус Concept продемонстрировал возможность использования макроязыков для создания самовоспроизводящихся макросов, включаемых в каждый из существующих и вновь создаваемых документов.

В 1996 году был разработан еще один макровирус – Laroux, первого вируса для Microsoft Excel. Далее за ними последовала целая череда вирусов, использующая уязвимости различных программ пакета Microsoft Office.

Этот новый тип вирусов был достаточно опасным в силу ряда причин:

1. массовое распространения среды существования вируса – документы и файлы, которые созданы в приложении, поддерживающем макросы. Такие

как документы MS Office и другие самые популярные приложения, например, Corel.

2. использование языка высокого уровня,

3. возможность передачи различными способами (через вложения к электронной почте и мобильные носители информации),

4. кроссплатформенность, т.к. макровирусы не используют уязвимости в каких–то определенных ОС, а зависят от среды исполнения, программы, поддерживающей выполнение макросов.

В течение нескольких следующих лет макровирусы вытеснили остальные типы вирусов, став наиболее распространенными. Ситуация изменилась только к 2002 году, когда их количество постепенно начало снижаться [11], что было обусловлено появлением механизмов защиты встроенных в Microsoft Office 2000, блокировавших выполнение макросов. А также технологий антивирусной защиты, позволявших выявить макровирусы еще до их выполнения. В результате, макровирусы полностью перестали существовать в 2008 году.

Почтовые вирусы

В 1999 году случилась еще одна крайне обширная вирусная эпидемия, вызванная вирусом Melissa, распространяющимся через адресную книгу Microsoft Outlook. Пользователь собственноручно запускал этот вирус на свой компьютер, открывая вложение к письму, содержащее макрос. Вирус Melissa был первым почтовым червем. За его создание разработчик получил наказание в виде 20 месяцев тюремного заключения и штрафа в 5000 долларов.

В 2000 году распространение вируса «ILOVEYOU» или «Love Bug» привело к ущербу мировой экономике в размере около 15 миллиардов долларов, сегодня он считается самым разрушительным вирусом из существующих. Вирус ILOVEYOU – это почтовый червь написанный на языке VBScript, распространяющийся через вложение к электронному письму. Автор червя использовал методы социальной инженерии, провоцируя пользователей открывать вложение к письму. Далее вирус распространял себя по всем контактам пользователя, всего заражению подверглись более 3 миллионов компьютеров по всему миру. ФБР удалось довольно быстро отследить место запуска вируса в сеть – Филиппины, и его автора. Однако отсутствие национального законодательства по борьбе с компьютерными преступлениями, и в том числе с созданием вирусов, привело к тому, что данное преступление осталось безнаказанным.

Именно вирус ILOVEYOU заставил мировое сообщество задуматься о создании единых общих межгосударственных законов о компьютерных преступлениях [11].

Компьютерные взломы

В этот период произошло несколько крупных взломов компьютерных систем в банковских и государственных организациях, среди которых особенно выделяются взломы Citibank и компьютерных систем Министерства Обороны США.

Владимир Левин и Citibank

В 1995 году в аэропорте Лондон Хитроу Интерполом был задержан Владимир Левин, возглавлявший группу хакеров, которые взломали компьютерные системы Citibank и похитили около 10 миллионов долларов. Деньги были переведены на зарубежные счета, в частности в банках Финляндии и Израиля.

Левин был экстрадирован в США, где ему было предъявлено обвинение. В результате судебных разбирательств Левин был приговорен к трём годам лишения свободы и возмещению ущерба Ситибанку в размере 240 015 долларов (его доля от украденных средств).

Арест Левина, как и совершенное им ограбление, стали одним из самых громких событий 1990–х годов.

Взлом МО США

В 1998 году хакерами (подростки из США) под руководством Эхуда Тененбаума (Analyzer), гражданина Израиля, были взломаны компьютеры МО США. Изначально военные связывали эту атаку с обострением ситуации в Персидском заливе, однако позже эта версия была опровергнута. Хакеры использовали известную уязвимость ОС Solaris. Эхуд Тененбаума избежал наказания.

Компьютерное мошенничество и угрозы электронной коммерции

Рост популярности систем онлайн торговли, переход на системы электронной коммерции и перевод банковских услуг в Интернет не могли не спровоцировать рост хакерской активности в данных областях.

К началу периода во всех развитых странах кредитные карты были абсолютно привычным явлением, и уже к началу 2000–х онлайн платежи также стали достаточно популярны.

Примерно в середине 1990–х обострилась проблема, связанная с мошенничеством с кредитными картами. В 1995 году ущерб от мошенничества составил порядка 1,63 миллиарда долларов. Существующие способы борьбы не были достаточно эффективными, меры противодействия, в том числе законодательные, также являлись недостаточными.

Спам

Считается, что несколько случаев массовой рассылки писем и даже телеграмм произошли еще до эры ПК и Интернета.

В середине 1990–х началось победоносное шествие такого явления как спам по просторам сетей. Толчком к созданию и развитию спам–технологий и спам–ботов стала программа, призванная защищать пользователей USENET от нежелательных рассылок. Приложение для модераторов – Automated Retroactive Minimal Moderation (ARMM), позволяющее просматривать и блокировать сообщения пользователей до публикации, содержало ошибку. Сообщение, отклоненное модератором, отправлялось на адрес группы USENET бесконечное число раз.

Первым известным случаем массовой рассылки нежелательных рекламных объявлений с использованием специального скрипта, первого спам–бота, по различным группам в сети USENET, является рассылка инициированная Лоуренсом Кантером и Мартой Сигел. Фактически эта пара открыла новую технологию продвижения собственного товара, попутно создав одну из основных проблем безопасности 21 века – спам.

Количество спам сообщений росло экспоненциально, если в 2001 году процент спама от всего почтового трафика составлял всего лишь 8%, то к концу периода (2004 году) количество спама достигло отметки в 72%. Достигнув своего пика в 2010 году – 89%, процент спама постепенно стал снижаться.

Развитие Интернета и рост числа обычных пользователей, не являющихся компьютерными специалистами, привели к тому, что во второй половине 1990–х получил развитие новый вид угроз – фишинг (в т.ч. «нигерийские письма» и мошенничество с лотереей), когда злоумышленник пытается похитить персональную, финансовую информацию или пароли, или же, используя методы социальной инженерии, вынуждает пользователя к совершению необходимого злоумышленнику действия (открытие ссылки, скачивание вложения к письму).

Отказ в обслуживании

Считается, что первые атаки на отказ в обслуживании были произведены относительно давно, но именно в этот период они получили максимальное развитие. Отсчет «классическим» DoS и DDoS атакам начинается в 1996 году Эти атаки были совершены с помощью отправки «почтовых бомб» на адреса нескольких тысяч списков рассылки, в результате несанкционированных рассылок подписчик получал порядка 100 000–1 000 000 писем ежедневно. Данные атаки были возможны, в силу того, что при оформлении подписки не требовалось прохождение аутентификации, и злоумышленник просто добавлял в списки новые и новые адреса. Целью атаки злоумышленник называл желание повысить уровень безопасности и требование введения процедуры аутентификации и подтверждения запроса на подписку на сетевых ресурсах.

Также в 1996 году была произведена первая другого типа – флуд атака, получившая огласку. Атаке подвергся крупнейший Интернет–провайдер Нью–Йорка. Это была атака типа SYN Flood, в которой с рандомных IP–адресов создается запрос на подключение (с использованием SYN пакетов, порядка 150 в секунду) к серверу, все пакеты доставляются получателю, и, т.к. при получении анализируется только адрес отправителя, сервер начинает соединение по каждому их запросов, резервирует под него место, отправляет пакет–подтверждение и начинает ожидать пакет в ответ. Множество подобных соединений полностью парализуют работу сервера.

В начале 1998 года, появились первые сообщения о проведении DDoS атак с помощью различных средств автоматизации и специальных программных инструментов. В открытом доступе в Интернете появилось большое количество инструментов для DDos атак: Fapi, Trinoo, TFN (Tribal Flood Network), Stacheldraht, Mstream, Omega, Trinity, Derivatives, myServer, Plague [13].

В результате развития технологий DDoS и доступности готовых инструментов, в 2000 году 15–летний хакер под ником MafiaBoy запустил одну из крупнейших DDoS атак, направленную на сайты eBay, CNN, Yahoo и Amazon. Эта атака явно продемонстрировала уязвимости и слабую степень защиты даже на сайтах крупнейших ИТ–компаний. В результате атаки были понесены многомилионные убытки, связанные с восстановлением доступности своих систем, а также с потерей доверия от пользователей, опасающихся производить электронные покупки через их сайты (не достаточно защищенные для оплаты по кредитным картам).

Начиная с 2002 года DDoS атаки набирают популярность, и постепенно становятся самыми распространенными и опасными. Атаки

подобного типа получили широкое распространение благодаря тому, что они направлены на нарушение доступности конкретных сервисов или ресурсов защиты, и из–за этого достаточно легко реализуемы.

Сегодня DDoS атаки, в основном, это орудие хакеров–шантажистов и политически или идеологически ориентированных хакеров и кибертеррористов.

Часто DDoS атаки направлены на сам Интернет, а точнее на вывод из строя участка сети, путем произведения атак на аккумулирующие или центральные маршрутизаторы и коммутаторы, или на серверы систем доменных имен (DNS) Интернет–провайдеров, а не на какой–то конкретный сайт [14].

В октябре 2002 года была произведена мощная DDoS атака, которая вывела из строя 8 из 13 корневых серверов DNS. Несмотря на то, что атака не имела серьезных последствий и сильно не нарушила работу сети, она продемонстрировала уязвимость корневых DNS перед атаками этого типа.

Защита информации в период с 1994 года до начала 2000–х

Криптография, новые стандарты и технологии

В начале 1990–х криптография развивалась в основном благодаря ИТ–компаниям, занимающимся поиском новой единой технологии безопасной передачи данных через Интернет.

Компанией RSA Security был разработан стандарт S/MIME (Secure Multipurpose Internet Mail Extensions), для обеспечения криптографической безопасности электронной почты.

Вышедший в 1994 году первый Интернет–браузер Netscape уже реализовывал стандарт шифрования SSL (также разработка компании Netscape Communications), для аутентификации и обеспечения конфиденциальности и целостности сообщений.

Стандарт SSL также основан на использовании открытых ключей, что позволяло обеспечивать целостность и конфиденциальность передаваемых данных. SSL, встроенный в браузер, позволял производить безопасный обмен такой информацией, как данные кредитных карт и прочей критически важной информацией.

В CommerceNet была разработана безопасная версия протокола HTTP – S–HTTP, для шифрования соединений по HTTP. Протокол HTTPS появился несколько позже и был поддержан основными игроками рынка ИТ – Microsoft и Netscape.

До 1996 года в США существовали законы, запрещающие экспорт ПО и оборудования с криптографической защитой, использующей ключи длиной более 40 бит. Разработчики были вынуждены создавать 2 версии – для внутреннего рынка и для

экспорта. В 1996 году вышли поправки к законам, позволяющие использовать более длинные ключи в 56 бит. Позже ограничения на экспорт и использование криптографических технологий с длинными ключами были сняты.

В этот период был разработан алгоритм AES (Advanced Encryption Standard). AES – это алгоритм блочного симметричного шифрования. Сегодня алгоритм AES применяется для защиты данных в правительственных и банковских организациях, для защиты беспроводных соединений, а также для защиты государственных данных США уровня «совершенно секретно».

Специализированное ПО

В данный период продолжают активно развиваться технологии программной защиты информации, происходит поиск новых научно–обоснованных технологий и методов защиты: обнаружения вирусов, предотвращения атак.

Рынок программных решений компьютерной безопасности сложился во многом благодаря таким компаниям как RSA Data Security, Symantec, MacAfee, которые вели собственные разработки в интересах обычных пользователей и компаний. Увеличение внимания к проблеме безопасности среди таких крупных компаний как IBM, Microsoft, Cisco, и, как следствие, увеличение затрат на эти исследования привело к развитию и появлению новых программных и программно–аппаратных решений. Исследования и разработки по новым коммерческим продуктам велись совместно научным и коммерческим сообществом, что позволило создать гораздо более эффективные решения, чем те, которые разрабатывались в закрытых организациях.

Именно переход от закрытых разработок по заказу правительства к свободной разработке привело к новому качественному росту и развитию технологий компьютерной защиты. Данный факт во многом обусловлен тем, что в военных и правительственных организациях основной угрозой является угроза конфиденциальности информации, тогда как в коммерческих структурах важнее ее целостность.

Для решения задач защиты для государственных нужд было необходимо разрабатывать методы, основываясь на существующих правилах и протоколах работы с секретной информацией. Новые компьютерных технологии защиты разрабатывались с учетом сложившейся системы классификации секретной информации, принятых моделей управления доступом.

К концу периода рынок решений по компьютерной безопасности наполнился коммерческими коробочными антивирусными решениями и системами обнаружения вторжений.

Антивирусное программное обеспечение

Если технологии аутентификации и криптографии в основном развивались в ответ на запрос от крупных корпораций, занимающихся электронной торговлей, то производители антивирусных программ обратили свое внимание на растущий рынок персональных компьютеров. Именно в течение этих 10–ти лет определились лидеры и крупнейшие на сегодняшний день поставщики антивирусного программного обеспечения: Symantec, MacAfee, Kaspersky, Dr.Web.

В 1999 году в «Лаборатории Касперского» был разработан первый поведенческий блокиратор для макровирусов. В отличие от традиционных антивирусов, эта технология блокирует подозрительные действия, а не ищет оригинальную последовательность вирусного кода. Такой подход обеспечивает защиту как от известных, так и от неизвестных макровирусов.

Технологии поиска автора вируса и на сегодняшний день являются достаточно несовершенными. Например, практически невозможно отследить конкретного автора, если он запустил вирус из компьютера, находящегося в публичном доступе. Как правило, случаи успешного задержания автора связаны с тем, что разработчик оставил какие–то следы в коде, как автор вируса Melissa, или же вовсе собственное имя. Однако опытные разработчики вряд ли могут допустить подобные ошибки.

Межсетевые экраны

В 1994 году появился первый коммерческий межсетевой экран прикладного уровня. Шлюзы прикладного уровня позволяли как производить фильтрацию пакетов по заголовкам, так и работали на уровне приложений. Они способны перехватывать все пакеты, направляемые от или для определенных приложений. Такие межсетевые экраны позволяют фильтровать трафик не по портам и адресам, а по создавшему его процессу, что позволило повысить антивирусную защиту.

Развитие Интернета и клиент–серверных технологий требовало также развития технологий организации защищенных соединений между ресурсами и данными компании, доверенными пользователями и партнерами, физически находящимися вне локальной сети. Данный фактор послужил толчком к развитию технологий «интранет» и «экстранет» – доверенной частной сети внутри компании и другой,

гораздо более защищенной, корпоративной сети, доступ к которой осуществляется из Интернета.

Именно развитие «экстранета» послужило толчком к развитию файерволлов – к ним добавляется ряд функций: шифрование, аутентификация пользователей, функции антивируса.

Крупные территориально распределенные компании нуждались в технологиях создания единой защищенной сети, на подобии локальной, между своими региональными офисами и партнерами. Решение было основано на использовании межсетевых экранов, позволяющих обеспечить туннелированние и организовать виртуальные частные сети.

Системы обнаружения вторжений

Подсоединение к Интернету коммерческих организаций, в которых имелась некоторая чувствительная информация, требовало применения дополнительных мер защиты.

В течение данного периода появилось достаточно большое число коммерческих систем обнаружения вторжений (Intrusion detecting systems, IDS). Это были экспертные системы, позволяющие сигнализировать о происходящих сетевых атаках.

В 1990–ых наиболее популярными сетевыми системами были Netranger (Wheelgroup, позже выкупленная Cisco) и Real Secure (Internet Security Systems).

История IDS начинается еще в 1980–ых годах, когда базовые идеи автоматизации обнаружения вторжений были представлены Джеймсом Андерсоном в работе, посвященной возможности применения результатов финансового аудита для выявления НСД к мейнфреймам. Перед исследователями того времени стояла задача определения перечня потенциальных угроз и атак, а также их особенностей и способов обнаружения в данных аудита.

В 1984–1986 годах Дороти Деннинг и Питером Нейманом была разработана первая система обнаружения вторжений IDES (Intrusion detection expert system), действующая в реальном времени. Система позволяла выявлять действия известного вредоносного ПО и НСД. Эти IDS являлись экспертными системами, основанными на правилах, и действовали на основании статистических методов. Они были призваны выявлять некоторую подозрительную или вредоносную активность анализируя сетевой трафик и данные приложений пользователей. Именно из этих исследований родились современные системы обнаружения вторжений [15]. В течение нескольких следующих лет появились IDS, в которых реализовывались новые,

более совершенные методы выявления атак. Например, в системе NIDES (1993 год) применялись нейронные сети.

Другой тип IDS, появившийся в этот период, это системы, основанные на знании. Они производят детектирование атак, основываясь на сигнатурном анализе процессов компьютерной системы или анализе сетевого трафика. Основным недостатком является то, что они неэффективны против новых атак, необходимо постоянное обновление и, возможно, обучение их новым сигнатурам.

Последний тип систем, разработанных в этот период, основывался на анализе поведения, позволяя выявлять новые, еще неизвестные типы атак. Такие системы позволяли выявлять аномальное поведение на пользовательских станциях.

Однако, сетевые IDS обладают одним большим недостатком – ограничение скорости анализа трафика. В 2001 году максимальная скорость составляла всего 1 Гигабит/сек (125 Мбайт/сек). Развитие технологий связи и увеличение скорости передачи данных привели к тому, что достаточно быстро сетевые IDS утратили свою актуальность.

Для решения проблемы скоростей исследователи и разработчики обратились к развитию узловых IDS, позволяющих анализировать данные на хосте и также выявлять атаки. Одна из первых подобных систем, SNORT, была разработана под UNIX в 1998 году, а в 2000 году портирована на Windows.

К концу периода в развитии систем IDS оставался ряд нерешенных проблем, наиболее важной из которых были DDoS атаки. На каждый из запросов к атакуемой системе IDS будет срабатывать и выводить оповещения, в результате чего работоспособность системы окажется нарушенной. Также и сама IDS может являться объектом DDoS атак.

Системы разграничения доступа

Модели разграничения доступа. Ролевое разграничение доступа

В течение этого периода продолжают активно развиваются модели разграничения доступа, удовлетворяющие требованиям коммерческих структур.

До 1992 года существовали два подхода к управлению доступом: дискреционный и мандатный, описанные в стандарте Common Criteria. Мандатное управление доступом в коммерческих системах не применялось.

Несмотря на то, что дискреционное уже использовалось во многих коммерческих операционных системах, таких как Windows 2000 Server и Windows NT, его реализация в новых системах была затруднена рядом факторов: децентрализованное хранение политик

управления доступом, сложность централизованного управления полномочиями и трудности соотнесения с административной моделью организации.

В ответ на эти сложности была разработана ролевая модель разграничения доступа, реализованная во всех современных ОС – Role–based access control (RBAC). Вообще, сама суть ролевого разграничения доступа является продолжением иерархической структуры организации, где каждой должности соответствуют определенные полномочия. Наборы прав привязываются к должностям сотрудников или же к их функциональным ролям [16].

Первые модели ролевого разграничения доступа начали появляться еще в 1970–х годах, но они были разработаны для достаточно простых компьютерных систем и к началу данного этапа уже полностью не отвечали существующим требованиям.

Ролевое разграничение доступа в современном виде произошло из универсальной модели ролевого управления доступом, разработанной Дэвидом Феррайоло и Ричардом Куном в 1992 году. В 1996 году модель была доработана Санди, в нее была включена возможность осуществления мандатного разграничения доступа. В 2004 модель Санди, Феррайоло и Куна была принята за единый стандарт.

Сегодня, некоторые эксперты считают, что ролевое разграничение доступа во многом изжило себя, и в противовес ему предлагаю использовать концепцию атрибутного управления доступом (Attribute–based access control (ABAC)) [17].

Программно–аппаратные системы разграничения доступа

В середине 1990–х RSA открыла новые возможности для электронных подписей и аутентификации.

В 1995 году на основании алгоритма RSA было разработана линейка продуктов RSA SecurID. Именно они положили начало развитию технологии двухфакторной аутентификации с использованием дополнительных технических устройств. Отсутствие единых государственных или отраслевых стандартов привело к тому, что RSA SecurID стал своеобразным эталоном производства подобных устройств. В дополнение к устройствам появилось и специализированное программное обеспечение, такое как Secursigth, для создания решений в масштабах предприятия.

До 2002 года, при организации удаленного доступа к внутренним ресурсам компании, идентификация пользователей производилась на основании предъявленных логина и пароля, однако существовала угроза перехвата передаваемых через Интернет данных и подмены

пользователя. Решение этой проблемы было предложено в компании RSA Security, которая первой предложила использовать для удаленного доступа двухфакторную идентификацию с использованием RSA SecurID, генерирующей дополнительный одноразовый пин–код.

Беспроводная связь, уязвимости и стандарты защиты

В 2000 году в широкой продаже появляются первые Wi–Fi устройства стандарта 802.11.

С развитием технологий беспроводной связи развивались и технологии взлома. Появились Wi–Fi снифферы, позволяющие получить доступ, производя поиск незащищенных сетей.

Вторая серьезная опасность беспроводной связи – перехват трафика «на лету».

Для решения этой проблемы уже в первых устройствах применялся протокол безопасности WEP (Wired Equivalent Privacy). На данном этапе развития технологии Wi–Fi не применялось никаких процедур аутентификации и использовался крайне нестойкий алгоритм шифрования (алгоритм RC4). Вскоре после появления WEP появилось большое число публикаций, отражающих слабость криптографической защиты и выявляющих большое число уязвимостей.

В 2003 году вышла новая версия стандарта Wi–Fi и появились новые устройства, реализующие чуть более стойкие механизмы защиты — WPA (Wi–Fi Protected Access). WPA обеспечивает более качественное шифрование и аутентификацию, что позволяет лучше противодействовать перехвату и раскрытию трафика, обеспечивает лучшую безопасность данных и контроль доступа. В WPA используется протокол аутентификации EAP (Extensible Authentication Protocol) и шифрование TKIP (реализующий все тот же алгоритм RC4, но с дополнительными механизмами защиты). По сути, TKIP – это переходный этап, реализованный для обеспечения постепенного перехода между устройствами WEP и WPA. TKIP был призван решить проблему расшифровки трафика злоумышленником на старых устройствах WEP. Именно использование TKIP не позволяет использовать Wi–Fi на скоростях, превосходящих 54 Мбит/сек.

Спустя год, в 2004, появился обновленный протокол безопасности Wi–Fi – WPA2, в котором протокол TKIP заменен на CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) и AES (Advanced Encryption Standard). Протокол AES, в отличие от TKIP, является самостоятельным серьезным алгоритмом шифрования, применяющимся в правительственных системах связи. AES являлся сертифицированным стандартом шифрования для применениях в системах обработки конфиденциальных документов, он

был включен в WPA2 именно для того, чтобы появилась возможность применения Wi–Fi в правительственных и военных сетях. Скорость его работы также является заметно более высокой, что позволяет эффективно его применять для сетей беспроводной связи.

В 2003 году, независимо от других разработок, в Китае был разработан собственный стандарт беспроводной связи WAPI (WLAN Authentication and Privacy Infrastructure). Использование этого стандарта вызвало большое число критических заявлений и осуждения.

В период 2008–2010 годов был опубликован ряд работ, посвященных уязвимостям в WPA и WPA2, в частности в WPA–TKIP. На сегодняшний день существует ряд известных уязвимостей, через которые возможна реализация атак.

4 этап: вторая половина 2000–х – настоящее время

Новые технологии и угрозы

Последний этап развития компьютерных преступлений и программно–аппаратных средств защиты информации начался примерно в середине 2000–х годов. Его начало связано с повсеместным распространением Интернета и социальных сетей, появлением доступных мобильных устройств (смартфоном, планшетов), развитием технологий мобильной и беспроводной связи.

Новые технологии порождают как новые виды угроз, так и ведут к трансформации и актуализации старых.

Миниатюризация и повсеместное распространение мобильных и переносных устройств привели к тому, что сегодня крайне опасной является их кража или потеря. Эти проблемы актуальны как для индивидуальных пользователей, т.к. их личные устройства хранят персональную информацию и платежные данные, так и для различных организаций, т.к. часто сотрудники используют корпоративные устройства вне периметра защиты. Утрата такого устройства может привести к крупным финансовым потерям, а также к ущербу репутации компании. Единственным способом защитить свою информацию в этом случае является полное шифрование данных.

На современном этапе, согласно статистике, наиболее распространенными являются:

- DDoS–атаки,
- атаки на мобильные устройства,
- атаки через уязвимости приложений и компонентов операционных систем,
- SQL инъекции.

Наибольшую опасность представляют таргетированные атаки различных типов и инсайдеры.

Существенно снизилось число вирусных атак [18]. Однако, эта угроза также не перестает быть актуальной, меняются только цели атаки и используемые уязвимости.

Социальные сети

Интенсивное развитие и распространение средств инфокоммуникации привело к глобализации всех процессов развития общества, а также всех информационных процессов. Повсеместное распространение Интернета и средств массовой коммуникации(СМК): блогов, форумов, социальных сетей, приводит к тому, что объем

информации растет в геометрической прогрессии, вместе с этим растет и зависимость общества от этой информации.

Социальные сети, такие как Facebook, Instagram, Twitter, создали совершенно новый Интернет, типичным пользователем которого является школьник, подросток и домохозяйка. Это люди совершенно не знакомые ни с правилами безопасного поведения в Интернет, ни с какими–то технологиями защиты. Рост числа потенциальных жертв компьютерных преступлений ведет к тому, что и компьютерных преступников становится больше. Появляются новые типы компьютерных преступлений.

Веб–аудитория в России и во всем мире продолжает увеличиваться и по данным Минкомсвязи РФ на начало 2015 года составила 74 млн. человек — это около 62% населения России. Наиболее активными пользователями Интернет являются достаточно молодые люди, 70% самых активных пользователей «всемирной паутины» – это пользователи в возрасте 18–24–лет. Однако интерес к блогам и различным тематическим форумам одинаков среди всех возрастных групп. Тем самым подтверждается рост влияния содержимого различных веб–ресурсов на все группы населения.

Постепенно технология WWW трансформируется в Giant Global Graph (GGG) – гигантский глобальный граф взаимодействий пользователей Интернет, где пользователи выходят на новый уровень общения, создавая, обмениваясь и используя, индивидуально и коллективно, мультимедийную информацию.

Рост числа пользователей Интернет ведет к тому, что компьютерные преступления становятся поистине глобальными и охватывающими весь мир. Масштабы и скорость выполнения атак и совершения преступлений также поражают. Одна запущенная вирусная атака в течение суток может поразить миллионы пользователей по всему миру, то же касается и DDOS–атак – миллионы пользователей могут являться участниками такой атаки. Существует тенденция к увеличению случаев атак, направленных на индивидуальных пользователей.

Инсайдеры

Статистика последних лет подтверждает тот факт, что опасность внутренних угроз заметно выше внешних. Недостаточное распространение комплексных систем защиты от утечек и средств защиты от внутренних угроз в целом приводит к тому, что данные утекают регулярно и с угрожающей интенсивностью. Средний ущерб от одной утечки оказывается значительно выше, чем ущерб от атаки извне. Проблемы внешних атак стали актуальными еще в середине

девяностых. За прошедшее с тех пор время появилось большое число эффективных технологий и средств защиты, компании научились бороться и с хакерами, и с вирусами. Инсайдеры же до сих пор явление, изученное не всеми специалистами по информационной безопасности, а потому опасное вдвойне.

Согласно выводам экспертов, утечка 20% коммерческой информации в 60% случаев приводит к банкротству компании.

Инсайдеры являются внутренними источниками угроз – это субъекты, имеющие прямой доступ к штатному оборудованию и к техническим средствам объекта, подлежащего защите.

Причина возникновения внутренних угроз связана с необходимостью использования труда наемных рабочих и предоставления им каких–либо прав доступа к конфиденциальной информации – возникает вопрос доверия сотрудникам. Вследствие того, что любой человек материально ориентирован, всегда существует опасность хищения информации для получения выгоды. Но не только этот фактор является опасным, угрозу также представляет халатность сотрудников.

В классификации внутренних угроз в первую очередь можно выделить две большие группы: совершаемые из корыстных или других злонамеренных соображений, и совершаемые без злого умысла, по неосторожности или технической некомпетентности. Т.е. их можно разделить на злонамеренный и непредумышленный инсайд. Умышленные утечки чаще всего происходят через Интернет, а случайные – в результате потери или кражи оборудования.

Сегодня одна из основных задач программно–аппаратной защиты информации сводится к тому, что необходимо обеспечить привычные для сотрудника условия работы и уровень информационного обмена, и в тоже время обеспечить изолированность и безопасность защищаемой информации или компьютерной системы.

Индустрия 4.0 и киберфизические системы

Внедрение информационных систем в промышленность и управление производством также порождает ряд специфических угроз:

- проникновение в компанию,
- проникновения в ERP/MES,
- получение доступа в промышленную сеть,
- подключение к контроллерам управления.

Таблица 2. Угрозы киберфизических систем и предпосылки их формирования

Предпосылки	Угрозы
Новая архитектура, увеличение общего числа новых киберфизических систем с разными критериями безопасности	1. Угрозы безопасности функциональных узлов «Индустрии 4.0» 2. Угрозы безопасности полевых устройств в условиях ограниченной функциональности. 3. Атаки по сторонним каналам.
Новые технологии передачи данных Новые протоколы передачи данных Новые требования к обеспечению доступности данных «Индустрии 4.0»	4. Угрозы безопасности сетей передачи информации «Индустрии 4.0» 5. Угрозы безопасности при взаимодействии с функциональными узлами «Индустрии 4.0» посредством удаленного доступа. 6. Угрозы целостности информации при построении распределенных сенсорных сетей
Новые стандарты безопасности «Индустрии 4.0» Несовершенство организационных мер обеспечения безопасности применительно к «Индустрии 4.0»	7. Угрозы облачных вычислений в «Индустрии 4.0»
Новые системы и методы хранения данных Новые распределенные файловые системы Новые методы обработки данных	8. Угрозы системам хранения и обработки данных согласно требованиям к доступности в «Индустрии 4.0» 9. Угрозы целостности и конфиденциальности данных в распределенных системах хранения и обработки информации.

Новая архитектура и новые технологии приводят к возникновению новых угроз. Комбинированный подход к применению

программно–аппаратных средств защиты в «Индустрии 4.0» позволит поднять уровень защищенности на необходимый уровень, построить защиту от большинства угроз, но в большинстве случаев этого недостаточно для обеспечения защиты от третированных атак. Считается, что наиболее актуальными угрозами в «Индустрии 4.0» в России являются компрометация импортного программного обеспечения и оборудования и третированные атаки.

Как и везде, в «Индустрии 4.0» основными рисками являются люди, процессы и технологии, поэтому необходимо разрабатывать новые методы и подходы к защите от третированных атак в условиях внедрения технологий «Индустрии 4.0». Основное отличие от «Индустрии 3.0» является применение технологии быстрой передачи информации по беспроводным каналам связи (сети 5G), применение технологий хранения и обработки больших объемов данных, машинного обучения, автоматизированных систем управления, облачных технологий, моделирования всех технологических процессов. Все эти технологии позволяют достигать повышения эффективности предприятий и иных сфер деятельности человека.

Internet of Things

В последние несколько лет появилась такая новая проблема, как безопасность Интернета вещей (Internet of Things). Сегодня Интернет распространен практически повсеместно, через Интернет реализованы возможности удаленного управления бытовыми приборами, инженерными сетями, автомобилями и даже медицинскими устройствами и оборудованием. Интернет нашел новое применение, перенеся угрозы и уязвимости в совершенно новую среду, из виртуального пространства в реальное. Исследования по взлому привычных нам вещей становятся популярной темой на ведущих мировых конференциях по безопасности. Ведь если злоумышленники начнут пользоваться такими уязвимостями, это будет представлять серьезную опасность для здоровья и жизни пользователей [19].

Появляется такое новое явление как терроризм Интернета вещей (IoT Terrorism) [20].

Безопасность медицинских информационных систем

Помимо классических угроз и известных уязвимостей, медицинское оборудование и устройства подвержены совершенно новым типам угроз, в силу особенностей их работы. Являясь киберфизической системой, такие устройства имеют возможность физического воздействия на здоровье человека.

Специализированное медицинское оборудование и устройства, такие как беспроводные активные медицинские имплантируемые устройства и телеманипуляторы, обладают рядом особенностей, которые делают невозможным применение большинства стандартных технологий защиты. В частности, активные имплантируемые устройства, требуют «не инвазивных» средств защиты, которые не влияют на работу самого устройства. Мониторинг и оценка безопасности также должны осуществляться без воздействия на текущее функционирование устройства. Слабые вычислительные мощности делают невозможным применение в них существующих программно–аппаратных и криптографических решений.

В медицинских информационных системах, системах мониторинга, в диагностическом оборудовании и системах жизнеобеспечения пациента необходимо применение комплексного, проактивного и предупреждающего подхода к обеспечению информационной безопасности.

Направления развития систем информационной и кибер безопасности

Основные направления развития систем информационной и кибербезопасности:

- Разработка моделей и методов обеспечения безопасности функциональных узлов.
- Адаптация криптографических примитивов для использования в производственных и киберфизических системах.
- Разработка методов аудита киберфизических систем.
- Построение предиктивных систем защиты от новых угроз.
- Разработка моделей динамической оценки рисков безопасности киберфизических систем.
- Разработка методов аудита киберфизических систем на наличие уязвимостей к атакам по сторонним каналам.
- Разработка эффективных реализаций легковесной криптографии для новых технологий.
- Построение отказоустойчивых систем хранения и обработки данных.
- Разработка системы обеспечения целостности и конфиденциальности данных в распределенных системах хранения и обработки информации.
- Разработка новых конструкций помехоустойчивых кодов для распределенных систем хранения и обработки информации.

Каналы реализации угроз и современные программно–аппаратные средства защиты информации

Выделяют следующие основные способы реализации угроз и каналы утечек информации:

1. Внешние угрозы:
   - через НСД и (или) воздействие на объекты на аппаратном уровне;
   - через НСД и (или) воздействие на объекты на общесистемном уровне;
   - через НСД и (или) воздействие на объекты на прикладном уровне;
   - через НСД и (или) воздействие на объекты на сетевом уровне;
   - через физический НСД и (или) воздействие на линии (каналы) связи, технические средства, машинные носители информации;
   - через воздействие на пользователей, администраторов безопасности, администраторов информационной системы или обслуживающий персонал (социальная инженерия) [21].
2. Внутренние угрозы:
   - Мобильные устройства;
   - Съемные носители;
   - Интернет;
   - Электронная почта;
   - Кража/потеря оборудования;
   - Бумажные документы.

Для защиты от угроз различных типов на современном этапе применяются следующие основные технологии защиты:

1. Идентификация и аутентификация пользователей (в том числе многофакторная и биометрическая);
2. Программно–аппаратные системы разграничения доступа;
3. Программно–аппаратные средства криптографической защиты информации;
4. Аппаратно–программные средства защиты от НСД (электронные замки);
5. Программно–аппаратные средства организации безопасного сетевого взаимодействия и удаленного доступа;
6. Средства управления мобильными устройствами;
7. Аппаратно–программные средства защиты от утечек (DLP системы);

8. Аппаратно–программные средства обнаружения и предотвращения вторжений (IPS/IDS).

Библиография

1. Breen C., Dahlbom C.A. Signaling Systems for Control of Telephone Switching 1960. URL: http://www.historyofphonephreaking.org/docs/breen1960.pdf
2. История компьютерного андеграунда:Зарождение фрикинга 2003. URL: https://bugtraq.ru/library/underground/underground2.html (дата обращения: 03.08.2016).
3. Аверченков В.И. Р.М.Ю..К.Г.В..Р.М.В. Системы защиты информации в ведущих зарубежных странах: учеб. пособие для вузов. Брянск: БГТУ, 2007. 225 с.
4. История компьютерного андеграунда:Хакеры 80–х 2003. URL: https://bugtraq.ru/library/underground/underground4.html (дата обращения: 05.08.2016).
5. ГОСТ Р ИСО/ТО 13569–2007: Финансовые услуги. Рекомендации по информационной безопасности.
6. Б. В.Т. Конфликт интересов при осуществлении брокерской деятельности на рынке ценных бумаг // Вестник Финансового университета, № 1, 2007. С. 123–131.
7. Ingham K. A History and Survey of Network Firewalls URL: https://www.cs.unm.edu/~treport/tr/02–12/firewall.pdf (дата обращения: 23.08.2016).
8. DeNardis L. A HISTORY OF INTERNET SECURITY // The History of Information Security: A Comprehensive Handbook, 2007. pp. 681–704.
9. Компьютерные вирусы: 50 любопытных фактов №1 // Журнал «Хакер». 2003. URL: https://xakep.ru/2003/12/04/20637/ (дата обращения: 08.18.2016).
10. Abhijit Belapurkar A.C.H.P.N.V.S.P.S.S. Distributed Systems Security: Issues, Processes and Solutions. 2009. 334 pp.
11. Kabay M.E. A Brief History of Computer Crime: An Introduction for Students 2008. URL: www.mekabay.com/overviews/history.pdf (дата обращения: 19.08.2016).
12. Grebennikov N. Keyloggers: How they work and how to detect them (Part 1) 2007. URL: https://securelist.com/analysis/publications/36138/keyloggers–how–they–work–and–how–to–detect–them–part–1/ (дата обращения: 22.08.2016).
13. Patrikakis C., Masikos M., Zouraraki O. Distributed Denial of Service Attacks // The Internet Protocol Journal, Vol. 7, No. 4, 2004.
14. АНАЛИТИЧЕСКИЙ МАТЕРИАЛ. БОРЬБА С АТАКАМИ DDoS URL: http://www.cisco.com/web/RU/products/ps5887/products_white_paper0900aecd8011e927_.html (дата обращения:

24.08.2016).
15. The History and Evolution of Intrusion Detection // SANS Institute. InfoSec Reading Room. URL: https://www.sans.org/reading–room/whitepapers/detection/history–evolution–intrusion–detection–344 (дата обращения: 25.08.2016).
16. Омельченко А. Управление доступом на основе ролей: преимущества, практика, особенности 2015. URL: http://www.realitsm.ru/2015/06/upravlenie–dostupom–na–osnove–rolej–preimushhestva–praktika–osobennosti/ (дата обращения: 30.08.2016).
17. RBAC is Dead – Now What? // he State of Security. News. Trends. Insights. 2015. URL: http://www.tripwire.com/state–of–security/security–data–protection/security–controls/rbac–is–dead–now–what/ (дата обращения: 05.09.2016).
18. July 2016 Cyber Attacks Statistics // HACKMAGEDDON. Information Security Timelines and Statistics. 2016. URL: http://www.hackmageddon.com/2016/08/18/july–2016–cyber–attacks–statistics/ (дата обращения: 05.09.2016).
19. Блог компании Яндекс И.б. Краткая история хакерства. Рассказ от руководителя информационной безопасности Яндекса 2014. URL: https://habrahabr.ru/company/yandex/blog/244559/ (дата обращения: 12.01.2017).
20. Alagarsamy V. IoT – The Next Level of Terrorism 2016. URL: https://www.linkedin.com/pulse/iot–next–level–terrorism–venkat–alagarsamy (дата обращения: 18.01.2017).
21. МЕТОДИКА ОПРЕДЕЛЕНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ (ПРОЕКТ) // ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ (ФСТЭК РОССИИ). 2015. URL: http://fstec.ru/component/attachments/download/812 (дата обращения: 18.01.2017).

УНИВЕРСИТЕТ ИТМО

Миссия университета – генерация передовых знаний, внедрение инновационных разработок и подготовка элитных кадров, способных действовать в условиях быстро меняющегося мира и обеспечивать опережающее развитие науки, технологий и других областей для содействия решению актуальных задач.

КАФЕДРА БЕЗОПАСНЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Кафедра Безопасные Информационные Технологии (БИТ) была создана в 1998 году по решению Федеральной службы по техническому и экспортному контролю (ФСТЭК) как базовая кафедра для подготовки квалифицированных специалистов по защите информации. Все выпускающиеся поколения специалистов, начиная с 2006 года и по сей день, отличаются высоким уровнем подготовки и обширными знаниями в сфере информационной безопасности.

В научно–преподавательский состав кафедры входят известные ученые, опытные преподаватели и практикующие специалисты ведущих компаний отрасли информационной безопасности. Все они активно участвуют в исследовательских проектах в области защиты информации, среди которых выделяются такие направления как криптография и криптоустройства, исследование уязвимостей и защита от атак по сторонним каналам, компьютерная криминалистика, безопасность облачных технологий и распределенных систем, безопасность мультиагентных робототехнических систем, системы обнаружения вторжений, безопасность систем "Умный дом", мониторинг информационных потоков в открытых сетях (в том числе в Интернет) и идентификация пользователей в сети Интернет.

В лабораториях кафедры проводятся фундаментальные и прикладные научные исследования, осуществляется разработка программных и программно–аппаратных средств защиты информации, инструментов компьютерной криминалистики.

Кафедра подготавливает бакалавров и магистров по направлению «Информационная безопасность». Широкий профиль подготовки, знание методов обеспечения информационной безопасности и средств защиты информации, практические навыки работы с современными техническими, программными и программно–аппаратными средствами защиты информации – все это позволяет выпускникам кафедры найти работу на производственных предприятиях, в подразделениях информационной безопасности, научно–исследовательских и инновационных организациях, а также в коммерческих структурах.

Воробьева Алиса Андреевна
Пантюхин Игорь Сергеевич

История развития программно–аппаратных средств защиты информации

Учебное пособие

В авторской редакции
Редакционно–издательский отдел Университета ИТМО
Зав. РИО Н.Ф. Гусарова
Подписано к печати
Заказ №
Тираж
Отпечатано на ризографе

Редакционно-издательский отдел
Университета ИТМО
197101, Санкт-Петербург, Кронверкский пр., 49