Тема 2. Понятие информационных угроз и их виды

1. Информационные угрозы, их виды, причины.
2. Вредоносные программы, их виды.
3. Компьютерные преступления, их виды.

1.Информационные угрозы, их виды, причины

Несмотря на предпринимаемые дорогостоящие методы, функционирование компьютерных информационных систем выявило наличие слабых мест в защите информации. Неизбежным следствием стали постоянно увеличивающиеся расходы и усилия на защиту информации. Однако для того, чтобы принятые меры оказались эффективными, необходимо определить, что такое угроза безопасности информации, выявить возможные каналы утечки информации и пути несанкционированного доступа к защищаемым данным.

Подчеркнем, что само понятие «угроза» в разных ситуациях зачастую трактуется по-разному. Например, для подчеркнуто открытой организации угроз конфиденциальности может просто не существовать - вся информация считается общедоступной (СМИ); однако в большинстве случаев нелегальный доступ представляется серьезной опасностью. Иными словами, угрозы, как и все в ИБ, зависят от интересов субъектов информационных отношений (и от того, какой ущерб является для них неприемлемым).

Итак, реализация угроз информационной безопасности заключается в нарушении конфиденциальности, целостности и доступности информации. Злоумышленник может ознакомиться с конфиденциальной информацией, модифицировать ее, или даже уничтожить, а также ограничить или блокировать доступ легального пользователя к информации. При этом злоумышленником может быть как сотрудник организации, так и постороннее лицо. Но, кроме этого, ценность информации может уменьшиться ввиду случайных, неумышленных ошибок персонала, а также сюрпризов, иногда преподносимых самой природой.

Классификация информационных угроз представлены на рис.4, 5.

Рис.4. Типы информационных угроз

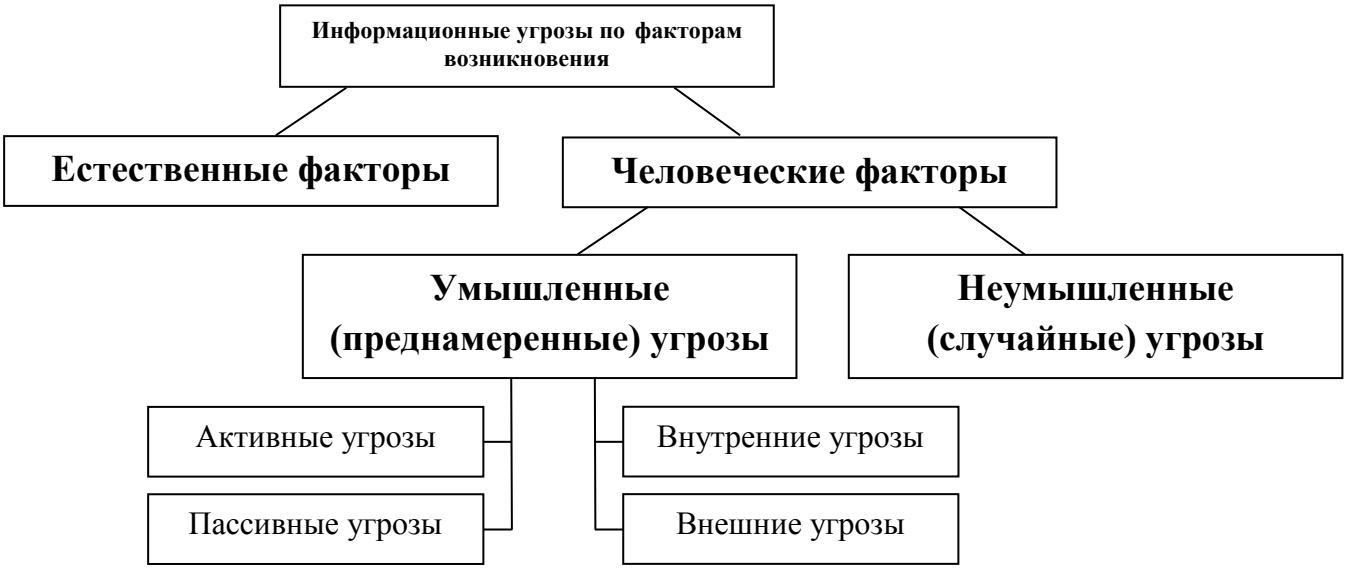


Рис.5. Классификация информационных угроз по факторам возникновения

Информационные угрозы могут быть обусловлены:

• естественными факторами (стихийные бедствия — пожар, наводнение, ураган, молния и другие причины);

• человеческими факторами. Последние, в свою очередь, подразделяются на:

- угрозы, носящие случайный, неумышленный характер. Это угрозы, связанные с ошибками процесса подготовки, обработки и передачи информации (научно-техническая, коммерческая, валютно-финансовая документация); с нецеленаправленной «утечкой умов», знаний, информации (например, в связи с миграцией населения, выездом в другие страны, для воссоединения с семьей и т.п.) Это угрозы, связанные с ошибками процесса проектирования, разработки и изготовления систем и их компонент (здания, сооружения, помещения, компьютеры, средства связи, операционные системы, прикладные пр01раммы и др.) с ошибками в работе аппаратуры из-за некачественного ее изготовления; с ошибками процесса подготовки и обработки информации (ошибки программистов и пользователей из-за недостаточной квалификации и некачественного обслуживания, ошибки операторов при подготовке, вводе и выводе данных, корректировке и обработке информации);

— угрозы, обусловленные умышленными, преднамеренными действиями людей. Это угрозы, связанные с передачей, искажением и уничтожением научных открытий, изобретений секретов производства, новых технологий но корыстным и другим антиобщественным мотивам (документация, чертежи, описания открытий и изобретений и другие материалы); подслушиванием и передачей служебных и других научно-технических и коммерческих разговоров; с целенаправленной «утечкой умов», знаний информации (например, в связи с получением другого гражданства по корыстным мотивам). Это угрозы, связанные с несанкционированным доступом к ресурсам автоматизированной информационной системы (внесение технических изменений в средства вычислительной техники и средства связи, подключение к средствам вычислительной техники и каналам связи, хищение носителей информации: дискет, описаний, распечаток и др.).

Умышленные угрозы преследуют цель нанесения ущерба пользователям АИС и, в свою очередь, подразделяются на активные и пассивные.

Пассивные угрозы, как правило, направлены на несанкционированное использование информационных ресурсов, не оказывая при этом влияния на их функционирование. Пассивной угрозой является, например, попытка получения информации, циркулирующей в каналах связи, посредством их прослушивания.

Активные угрозы имеют целью нарушение нормального процесса функционирования системы посредством целенаправленного воздействия на аппаратные, программные и информационные ресурсы. К активным угрозам относятся, например, разрушение или радиоэлектронное подавление линий связи, вывод из строя ПЭВМ или ее операционной системы, искажение сведений в базах данных либо в системной информации и т.д. Источниками активных угроз могут быть непосредственные действия злоумышленников, программные вирусы и т.п.

Умышленные угрозы подразделяются на *внутренние,* возникающие внутри управляемой организации, и *внешние.*

Внутренние угрозы чаще всего определяются социальной напряженностью и тяжелым моральным климатом.

Внешние угрозы могут определяться злонамеренными действиями конкурентов, экономическими условиями и другими причинами (например, стихийными бедствиями). По данным зарубежных источников, получил широкое распространение *промышленный шпионаж* - это наносящие ущерб владельцу коммерческой тайны, незаконный сбор, присвоение и передача сведений, составляющих коммерческую тайну, лицом, не уполномоченным на это ее владельцем.

К основным угрозам безопасности относят:

- раскрытие конфиденциальной информации;
- компрометация информации;
- несанкционированное использование информационных ресурсов;
- ошибочное использование ресурсов; несанкционированный обмен информацией;
- отказ от информации;
- отказ от обслуживания.

Средствами реализации угрозы *раскрытия конфиденциальной информации* могут быть несанкционированный доступ к базам данных, прослушивание каналов и т.п. В любом случае получение информации, являющейся достоянием некоторого лица (группы лиц), что приводит к уменьшению и даже потере ценности информации.

Реализация угроз является следствием одного из следующих действий и событий: разглашения конфиденциальной информации, утечки конфиденциальной информации и несанкционированный доступ к защищаемой информации (106). При разглашении или утечке происходит нарушение конфиденциальности информации с ограниченным доступом (рис. 6).

Рис. 6. Действия и события, нарушающие информационную безопасность

Утечка конфиденциальной информации - это бесконтрольный выход конфиденциальной информации за пределы ИС или круга лиц, которым она была доверена по службе или стала известна в процессе работы. Эта утечка может быть следствием:

- разглашения конфиденциальной информации;
- ухода информации по различным, главным образом техническим, каналам;
- несанкционированного доступа к конфиденциальной информации различными способами.

Разглашение информации ее владельцем или обладателем есть умышленные или неосторожные действия должностных лиц и пользователей, которым соответствующие сведения в установленном порядке были доверены по службе или по работе, приведшие к ознакомлению с ним лиц, не допущенных к этим сведениям.

Возможна *бесконтрольная утечка конфиденциальной информации* по визуально-оптическим, акустическим, электромагнитным и другим каналам.

По физической природе возможны следующие средства переноса информации:

- Световые лучи.
- Звуковые волны.
- Электромагнитные волны.

- Материалы и вещества.

Под каналом утечки информации будем понимать физический путь от источника конфиденциальной информации к злоумышленнику, по которому возможна утечка или несанкционированное получение охраняемых сведений. Для возникновения (образования, установления) канала утечки информации необходимы определенные пространственные, энергетические и временные условия, а также соответствующие средства восприятия и фиксации информации на стороне злоумышленника.

Применительно к практике с учетом физической природы образования каналы утечки информации можно разделить на следующие группы:

- визуально-оптические;
- акустические (включая и акустико-преобразовательные);
- электромагнитные (включая магнитные и электрические);
- материально-вещественные (бумага, фото, магнитные носители, производственные отходы различного вида - твердые, жидкие, газообразные).

К факторам утечки могут, например, относиться:

- недостаточное знание работниками предприятия правил защиты информации и непонимание (или недопонимание) необходимости их тщательного соблюдения;
- использование не аттестованных технических средств обработки конфиденциальной информации;
- слабый контроль за соблюдением правил защиты информации правовыми, организационными и инженерно-техническими мерами.

Несанкционированный доступ (НСД)

Это наиболее распространенный вид информационных угроз заключается в получении пользователем доступа к объекту, на который у него нет разрешения в соответствии с принятой в организации политикой безопасности. Обычно самая главная проблема определить, кто и к каким наборам данных должен иметь доступ, а кто нет. Другими словами, необходимо определить термин «несанкционированный».

По характеру, воздействия НСД является активным воздействием, использующим ошибки системы. НСД обращается обычно непосредственно к требуемому набору данных, либо воздействует на информацию о санкционированном доступе с целью легализации НСД. НСД может быть подвержен любой объект системы. НСД может быть осуществлен как стандартными, так и специально разработанными программными средствами к объектам.

Есть и достаточно примитивные пути несанкционированного доступа:

- хищение носителей информации и документальных отходов;
- инициативное сотрудничество;
- склонение к сотрудничеству со стороны взломщика;
- выпытывание;
- подслушивание;
- наблюдение и другие пути.

Любые способы утечки конфиденциальной информации могут привести к значительному материальному и моральному ущербу как для организации, где функционирует ИС, так и для ее пользователей.

Менеджерам следует помнить, что довольно большая часть причин и условий, создающих предпосылки и возможность неправомерного овладения конфиденциальной информацией, возникает из-за элементарных недоработок руководителей организаций и их сотрудников. Например, к причинам и условиям, создающим предпосылки для утечки коммерческих секретов, могут относиться:

- недостаточное знание работниками организации правил защиты конфиденциальной информации и непонимание необходимости их тщательного соблюдения;
- использование не аттестованных технических средств обработки конфиденциальной информации;
- слабый контроль за соблюдением правил защиты информации правовыми организационными и инженерно- техническими мерами и др.

Разглашение и утечка приводит к неправомерному ознакомлению с конфиденциальной информацией при минимальных затратах усилий со стороны злоумышленника. Этому способствуют некоторые не лучшие личностно-профессиональные характеристики и действия сотрудников фирмы, представленные на рис.7.

Рис. 7. Личностно-профессиональные характеристики и действия сотрудников, способствующие реализации угроз информационной безопасности

Обиженные сотрудники, даже бывшие, знакомы с порядками в организации и способны нанести немалый ущерб. Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа (логического и

физического) к информационным ресурсам аннулировались. Типы и субъекты информационных угроз представлены в табл.2.

Таблица 2

Типы и субъекты угроз

	Тип угроз	**Оператор**	**Руководитель**	**Программист**	**Инженер (техник)**	**Пользователь**	**Конкурент**
1.	Изменение кодов	+		+			
2.	Копирование файлов	+		+			
3.	Уничтожение файлов	+	+	+		+	+
4.	Присвоение программ			+	+		+
5.	Шпионаж	+	+	+			+
6.	Установка подслушивания			+	+		+
7.	Саботаж	+		+	+		+
8.	Продажа данных	+	+	+		+	
9.	Воровство		+	+		+	+

И даже если сотрудник не является злоумышленником, он может ошибаться не намеренно вследствие усталости, болезненного состояния и пр.

Ошибочное использование информационных ресурсов, будучи санкционированным, тем не менее, может привести к разрушению, раскрытию или компрометации указанных ресурсов. Данная угроза, чаще всего, является следствием ошибок в программном обеспечении АИС.

Уничтожение компьютерной информации - это стирание ее в памяти ЭВМ, удаление с физических носителей, а также несанкционированные изменения составляющих ее данных, кардинально меняющие содержание (например, введение ложной информации, добавление, изменение, удаление записей). Одновременный перевод информации на другой машинный носитель не считается в контексте уголовного закона уничтожением компьютерной информации лишь в том случае, если в результате этих действий доступ правомерных пользователей к информации не оказался существенно затруднен либо исключен.

Имеющаяся у пользователя возможность восстановить уничтоженную информацию с помощью средств программного обеспечения или получить данную информацию от другого пользователя не освобождает виновного от ответственности.

Уничтожением информации не является переименование файла, где она содержится, а также само по себе автоматическое "вытеснение" старых версий файлов последними по времени.

Блокирование компьютерной информации - это искусственное затруднение доступа пользователей к компьютерной информации, не связанное с ее уничтожением. Другими словами, это совершение с информацией действий, результатом которых является невозможность получения или использование ее по назначению при полной сохранности самой информации.

Компрометация информации, как правило, реализуется посредством внесения несанкционированных изменений в базы данных, в результате чего ее потребитель вынужден либо отказаться от нее, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений. В случае использования скомпрометированной информации потребитель подвергается опасности принятия неверных решений со всеми вытекающими последствиями.

Отказ от информации, в частности, непризнание транзакции (операции в банке) состоит в непризнании получателем или отправителем информации фактов ее получения или отправки. В условиях маркетинговой деятельности это, в частности, позволяет одной из сторон расторгать заключенные финансовые соглашения "техническим" путем, формально не отказываясь от них и нанося тем самым второй стороне значительный ущерб.

Модификация компьютерной информации - это внесение в нее любых изменений, кроме связанных с адаптацией программы для ЭВМ или базы данных. Адаптация программы для ЭВМ или базы данных - «это внесение изменений, осуществляемых исключительно в целях обеспечения функционирования программы для ЭВМ или базы данных на конкретных технических средствах пользователя или под управлением конкретных программ пользователя» (ч. 1 ст. 1 Закона РФ от 23 сентября 1992 года "О правовой охране программ для электронных вычислительных машин и баз данных"). Другими словами это означает изменение ее содержания по сравнению с той информацией, которая первоначально (до совершения деяния) была в распоряжении собственника или законного пользователя.

Копирование компьютерной информации - изготовление и устойчивое запечатление второго и последующих экземпляров базы данных, файлов в любой материальной форме, а также их запись на машинный носитель, в память ЭВМ.

Отказ в обслуживании представляет собой весьма существенную и распространенную угрозу, источником которой является сама АИС. Подобный отказ особенно опасен в ситуациях, когда задержка с предоставлением ресурсов абоненту может привести к тяжелым для него последствиям. Так, отсутствие у пользователя данных, необходимых для принятия решения, в течение периода, когда это решение еще может быть эффективно реализовано, может стать причиной его нерациональных действий.

Ниже перечисляются наиболее распространенные технические угрозы и причины, в результате которых они реализуются:

- несанкционированный доступ к информационной системе - происходит в результате получения нелегальным пользователем доступа к информационной системе;
- раскрытие данных - наступает в результате получения доступа к информации или ее чтения человеком и возможного раскрытия им информации случайным или намеренным образом;
- несанкционированная модификация данных и программ - возможна в результате модификации, удаления или разрушения человеком данных и программного обеспечения локальных вычислительных сетей случайным или намеренным образом;
- раскрытие трафика локальных вычислительных сетей - произойдет в результате доступа к информации или ее чтения человеком и возможного ее разглашения случайным или намеренным образом тогда, когда информация передается через локальные вычислительные сети;
- подмена трафика локальных вычислительных сетей - это его использование легальным способом, когда появляются сообщения, имеющие такой вид, будто они посланы законным заявленным отправителем, а на самом деле это не так;
- неработоспособность локальных вычислительных сетей - это следствие осуществления угроз, которые не позволяют ресурсам локальных вычислительных сетей быть своевременно доступными.

Способы воздействия угроз на информационные объекты подразделяются на:

- информационные;
- программно-математические;
- физические;
- радиоэлектронные;
- организационно-правовые.

К информационным способам относятся:

- нарушение адресности и своевременности информационного обмена, противозаконный сбор и использование информации;
- несанкционированный доступ к информационным ресурсам;
- манипулирование информацией (дезинформация, сокрытие или сжатие информации);
- нарушение технологии обработки информации.

Программно-математические способы включают:

- внедрение компьютерных вирусов;
- установка программных и аппаратных закладных устройств;
- уничтожение или модификацию данных в автоматизированных информационных системах.

Физические способы включают:

- уничтожение или разрушение средств обработки информации и связи;
- уничтожение, разрушение или хищение машинных или других носителей информации;

- хищение программных или аппаратных ключей и средств криптографической защиты информации;
- воздействие на персонал;
- перехват, дешифровка и навязывание ложной информации в сетях передачи данных и линиях связи;
- воздействие на парольно-ключевые системы;
- радиоэлектронное подавление линий связи и систем управления.

Радиоэлектронными способами являются:

- перехват информации в технических каналах ее возможной утечки;
- внедрение электронных устройств перехвата информации в технические средства и помещения;
- перехват, дешифровка и навязывание ложной информации в сетях передачи данных и линиях связи;
- воздействие на парольно-ключевые системы;
- радиоэлектронное подавление линий связи и систем управления.

Организационно-правовые способы включают:

- невыполнение требований законодательства о задержке в принятии необходимых нормативно-правовых положений в информационной сфере;
- неправомерное ограничение доступа к документам, содержащим важную для граждан и организаций информацию.

Суть подобных угроз сводится, как правило, к нанесению того или иного ущерба предприятию.

Проявления возможного ущерба могут быть самыми различными:

- моральный и материальный ущерб деловой репутации организации;
- моральный, физический или материальный ущерб, связанный с разглашением персональных данных отдельных лиц;
- материальный (финансовый) ущерб от разглашения защищаемой (конфиденциальной) информации;
- материальный (финансовый) ущерб от необходимости восстановления нарушенных защищаемых информационных ресурсов;
- материальный ущерб (потери) от невозможности выполнения взятых на себя обязательств перед третьей стороной;
- моральный и материальный ущерб от дезорганизации в работе всего предприятия.

Непосредственный вред от реализованной угрозы, называется воздействием угрозы.

Угрозы, исходящие от окружающей среды, весьма разнообразны. В первую очередь следует выделить нарушение инфраструктуры - аварии электропитания, временное отсутствие связи, перебои с водоснабжением, гражданские беспорядки и т. п. На долю огня, воды и аналогичных "врагов", среди которых самый опасный - низкое качество электропитания, приходится 13% потерь, которые обычно несут информационные системы.

Внешние субъекты могут быть случайными или преднамеренными и иметь

разный уровень квалификации. К ним относятся:

- криминальные структуры;
- потенциальные преступники и хакеры;
- недобросовестные партнеры;
- технический персонал поставщиков услуг;
- представители надзорных организаций и аварийных служб;
- представители силовых структур.

Внутренние субъекты, как правило, представляют собой высококвалифицированных специалистов в области разработки и эксплуатации программного обеспечения и технических средств, знакомы со спецификой решаемых задач, структурой и основными функциями и принципами работы программноаппаратных средств защиты информации, имеют возможность использования штатного оборудования и технических средств сети. К ним относятся:

- основной персонал (пользователи, программисты, разработчики);
- представители службы защиты информации;
- вспомогательный персонал (уборщики, охрана);
- технический персонал (жизнеобеспечение, эксплуатация).

Технические средства, являющиеся источниками потенциальных угроз безопасности информации, также могут быть внешними:

- средства связи;
- сети инженерных коммуникаций (водоснабжения, канализации);
- транспорт.

При взаимодействии интегрированной информационной системы управления предприятием с Internet основные угрозы для информационной безопасности организации представляют:

- несанкционированные внешние воздействия из Internetна информационную систему для получения доступа к ее ресурсам и (или) нарушения ее работоспособности;
- отказы аппаратного и программного обеспечения подсистемы взаимодействия (нарушение работы каналов связи с Internet, телекоммуникационного оборудования локальной вычислительной сети, межсетевых экранов);
- непреднамеренные действия сотрудников организации, приводящие к непроизводительным затратам времени и ресурсов, разглашение сведений ограниченного пользования через Internetили нарушению работоспособности подсистемы взаимодействия интегрированной информационной системы управления предприятием с Internet;
- преднамеренные действия сотрудников организации, приводящие к разглашению сведений ограниченного пользования через Internet, а также нарушение работоспособности подсистемы взаимодействия информационной системы с Internetили же недоступность предоставляемых услуг через Internet;

• непреднамеренные действия лиц, осуществляющих администрирование подсистемы взаимодействия интегрированной информационной системы управления предприятием с Internet, приводящие к разглашению сведений ограниченного пользования или нарушению взаимодействия с Internet;

• преднамеренные действия (в корыстных целях, по принуждению третьих лиц, со злым умыслом и т.п.) сотрудников организации, отвечающих за установку, сопровождение, администрирование системного, сетевого или прикладного программного обеспечения, технических средств защиты и обеспечения информационной безопасности подсистемы взаимодействия интегрированной информационной системы управления предприятием с Internet, которые (действия) приводят к разглашению сведений ограниченного пользования или нарушения взаимодействия с Internet.

Приводимая ниже классификация охватывает только умышленные угрозы безопасности автоматизированных информационных систем экономических объектов (АИСЭО), оставляя в стороне такие воздействия как стихийные бедствия, сбои и отказы оборудования и др. Реализацию угроз в дальнейшем будем называть атакой.

Угрозы безопасности можно классифицировать по следующим признакам:

1. По цели реализации угрозы. Реализация той или иной угрозы безопасности может преследовать следующие цели:

- нарушение конфиденциальной информации;
- нарушение целостности информации;
- нарушение (частичное или полное) работоспособности.

2. По принципу воздействия на объект:

- с использованием доступа субъекта системы (пользователя, процесса) к объекту (файлам данных, каналу связи и т.д.);
- с использованием скрытых каналов.

Под скрытым каналом понимается путь передачи информации, позволяющий двум взаимодействующим процессам обмениваться информацией таким способом, который нарушает системную политику безопасности.

3. По характеру воздействия на объект.

По этому критерию различают активное и пассивное воздействие.

Активное воздействие всегда связано с выполнением пользователем каких- либо действий, выходящих за рамки его обязанностей и нарушающих существующую политику безопасности. Это может быть доступ к определенным наборам данных, программам, вскрытие пароля и т.д. Активное воздействие ведет к изменению состояния системы и может осуществляться либо с использованием доступа (например, к наборам данных), либо как с использованием доступа, так и с использованием скрытых каналов.

Пассивное воздействие осуществляется путем наблюдения пользователем каких-либо побочных эффектов (от работы программы, например) и их анализе. На основе такого рода анализа можно иногда получить

довольно интересную информацию. Примером пассивного воздействия может служить прослушивание линии связи между двумя узлами сети. Пассивное воздействие всегда связано только снарушением конфиденциальности информации, так как при нем никаких действий с объектами и субъектами не производится. Пассивное воздействие не ведет к изменению состояния системы.

4. По причине появления используемой ошибки защиты.

Реализация любой угрозы возможна только в том случае, если в данной конкретной системе есть какая-либо ошибка или брешь защиты.

Такая ошибка может быть обусловлена одной из следующих причин:

- неадекватностью политики безопасности реальной системе. Это означает, что разработанная политика безопасности настолько не отражает реальные аспекты обработки информации, что становится возможным использование этого несоответствия для выполнения несанкционированных действий;

- ошибками административного управления, под которыми понимается некорректная реализация или поддержка принятой политики безопасности в данной организации. Например, согласно политике безопасности должен быть запрещен доступ пользователей к определенному набору данных, а на самом деле (по невнимательности администратора безопасности) этот набор данных доступен всем пользователям.

- ошибками в алгоритмах программ, в связях между ними и т.д., которые возникают на этапе проектирования программы или комплекса программ и благодаря которым их можно использовать совсем не так, как описано в документации. Примером такой ошибки может служить ошибка в программе аутентификации пользователя, когда при помощи определенных действий пользователь имеет возможность войти в систему без пароля.

- ошибками реализации алгоритмов программ (ошибки кодирования), связей между ними и т.д., которые возникают на этапе реализации или отладки и которые также могут служить источником недокументированных свойств.

5. По способу воздействия на объект атаки (при активном воздействии):

- непосредственное воздействие на объект атаки (в том числе с использованием привилегий), например, непосредственный доступ к набору данных, программе, службе, каналу связи и т.д., воспользовавшись какой-либо ошибкой. Такие действия обычно легко предотвратить с помощью средств контроля доступа.

- воздействие на систему разрешений (в том числе захват привилегий). При этом способе несанкционированные действия выполняются относительно прав пользователей на объект атаки, а сам доступ к объекту осуществляется потом законным образом. Примером может служить захват привилегий, что позволяет затем беспрепятственно получить доступ к любому набору данных и программе, в частности «маскарад», при котором пользователь присваивает себе каким-либо образом полномочия другого пользователя выдавая себя за него.

6. По объекту атаки. Одной из самых главных составляющих нарушения функционирования АИС является объект атаки, т.е. компонент системы, который подвергается воздействию со стороны злоумышленника. Определение объекта атаки позволяет принять меры по ликвидации последствий нарушения, восстановлению этого компонента, установке контроля по предупреждению повторных нарушений и т.д.

Воздействию могут подвергаться следующие компоненты:

- АИС в целом - злоумышленник пытается проникнуть в систему для последующего выполнения каких-либо несанкционированных действий. Для этого обычно используются метод «маскарада», перехват или подделка пароля, взлом или доступ к системе через сеть;

- объекты системы - данные или программы в оперативной памяти или на внешних носителях, сами устройства системы, как внешние (дисководы, сетевыеустройства, терминалы), так и внутренние (оперативная память, процессор), каналы передачи данных. Воздействие на объекты системы обычно имеет целью доступ к их содержимому (нарушение конфиденциальности или целостности обрабатываемой или хранимой информации) или нарушение их функциональности, например, заполнение всей оперативной памяти компьютера бессмысленной информацией или загрузка процессора компьютера задачей с неограниченным временем исполнения (нарушение доступности);

- субъекты системы - процессы и подпроцессы с участием пользователей. Целью таких атак является либо прямое воздействие на работу процесса - его приостановка, изменение привилегий или характеристик (приоритета, например), либо обратное воздействие - использование злоумышленником привилегий, характеристик и т.д. другого процесса в своих целях. Частным случаем такого воздействия является внедрение злоумышленником вируса в среду другого процесса и его выполнение от имени этого процесса. Воздействие может осуществляться на процессы пользователей, системы, сети;

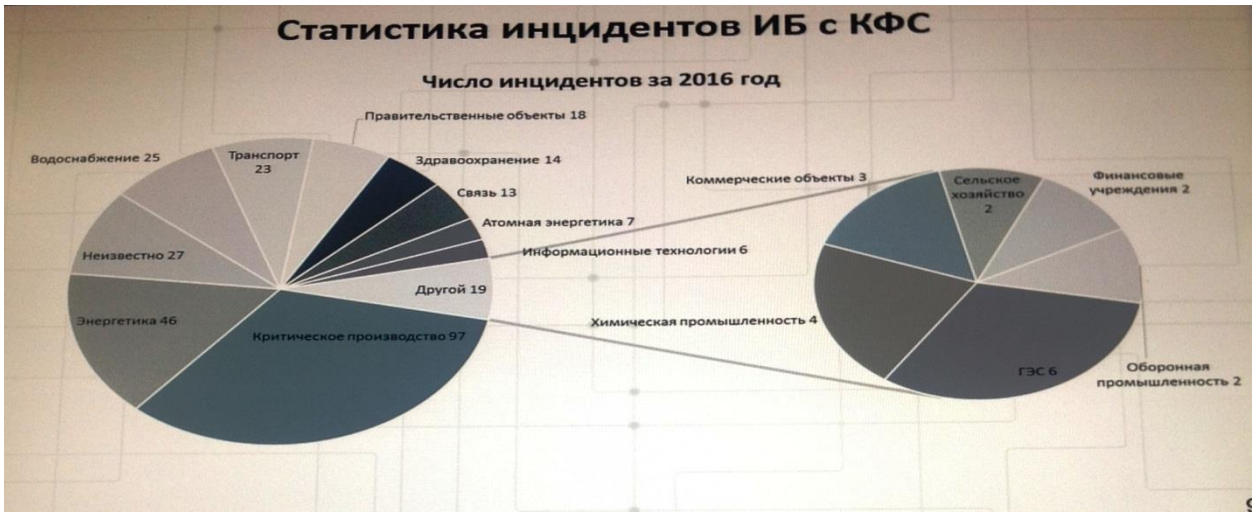
- каналы передачи данных - пакеты данных, передаваемые по каналу связи и сами каналы. Воздействие на пакеты данных может рассматриваться как атака на объекты сети, воздействие на каналы - специфический род атак, характерный для сети. К нему относятся: прослушивание канала и анализ трафика (потока сообщений) - нарушение конфиденциальности передаваемой информации; подмена или модификация сообщений в каналах связи и на узлах ретрансляторах - нарушение целостности передаваемой информации; изменение топологии и характеристик сети, правил коммутации и адресации - нарушение доступности сети.

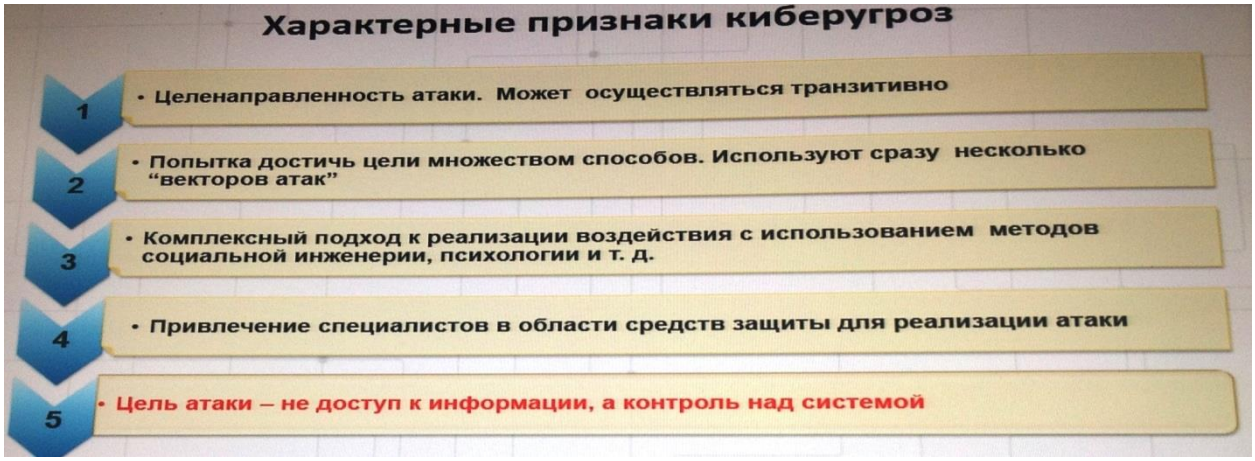
7. По используемым средствам атаки.

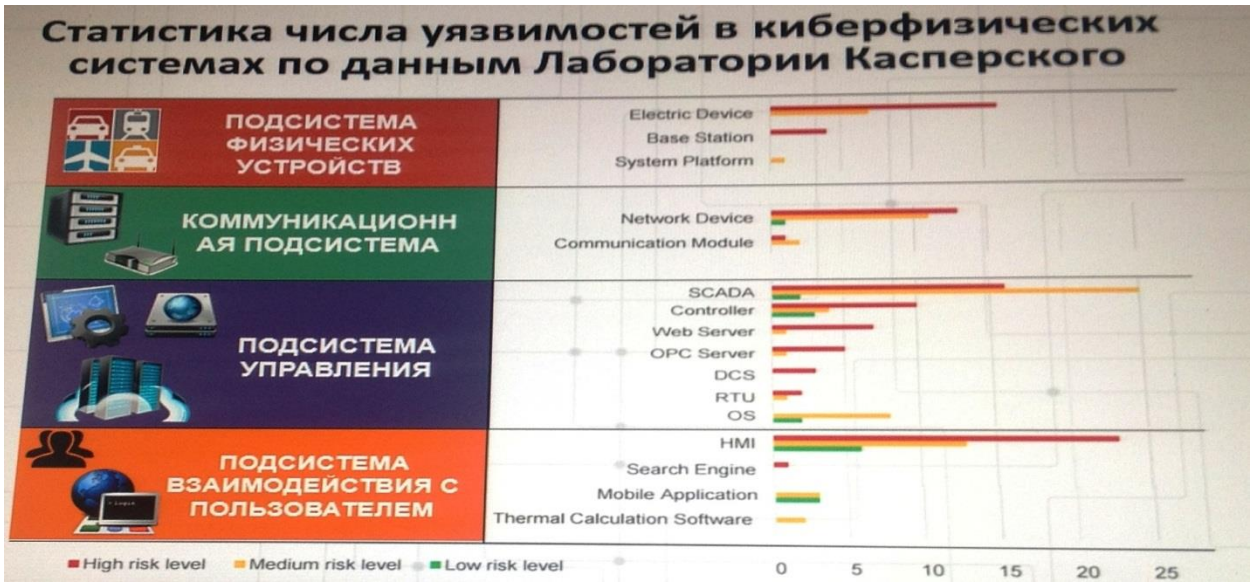
Для воздействия на систему злоумышленник может использовать стандартное программное обеспечение или специально разработанные программы. В первом случае результаты воздействия обычно предсказуемы, так как большинство стандартных программ системы хорошо изучены. Использование специально разработанных программ связано с большими

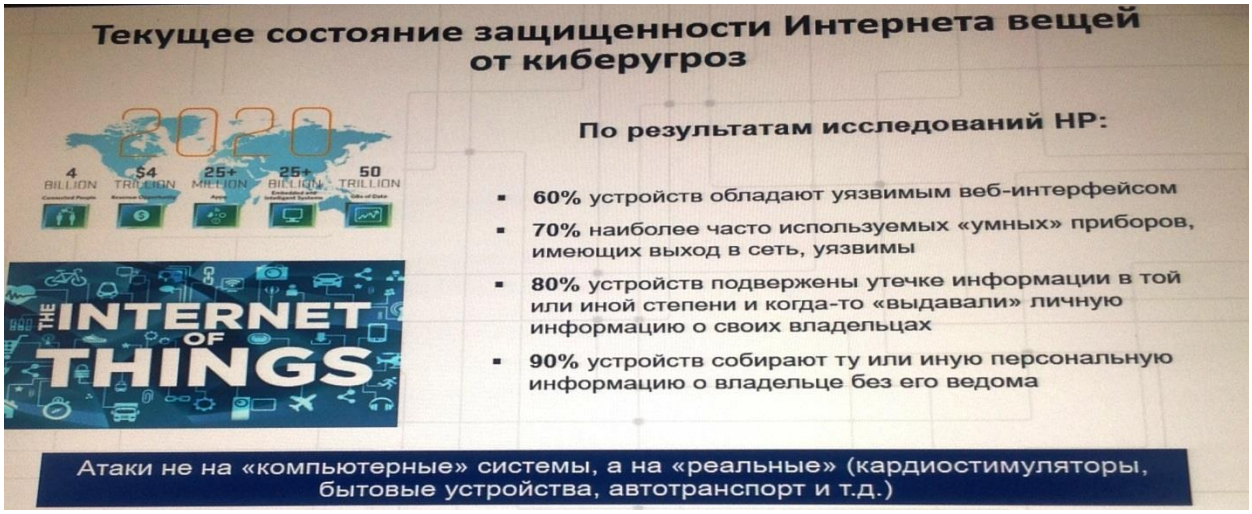
трудностями, но может быть более опасным, поэтому в защищенных системах рекомендуется не допускать добавление программ в АИСЭО без разрешения администратора безопасности системы.

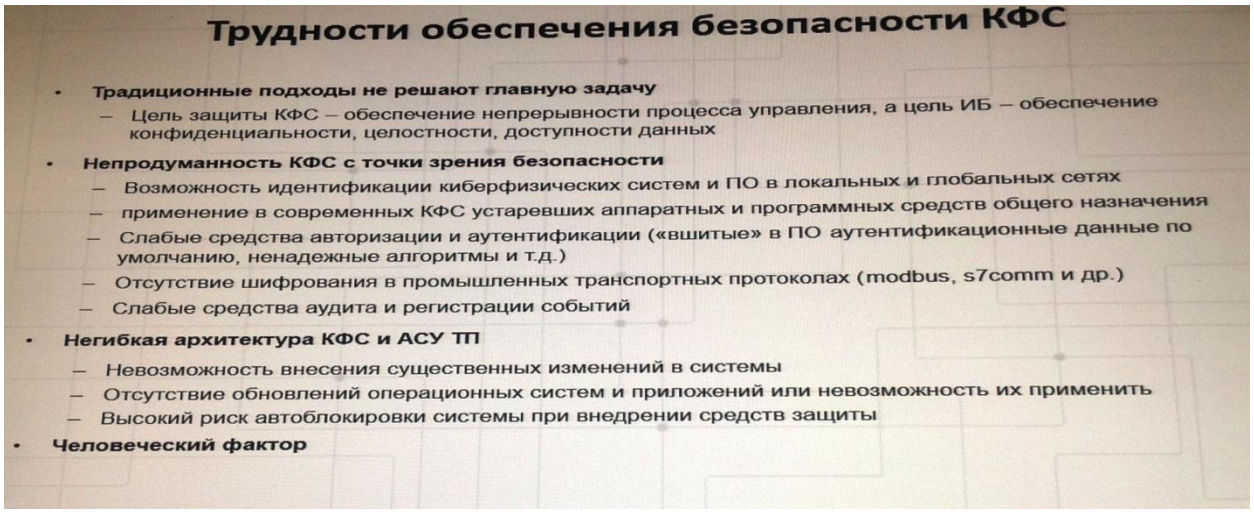
Дополнительный материал для самостоятельной работы.

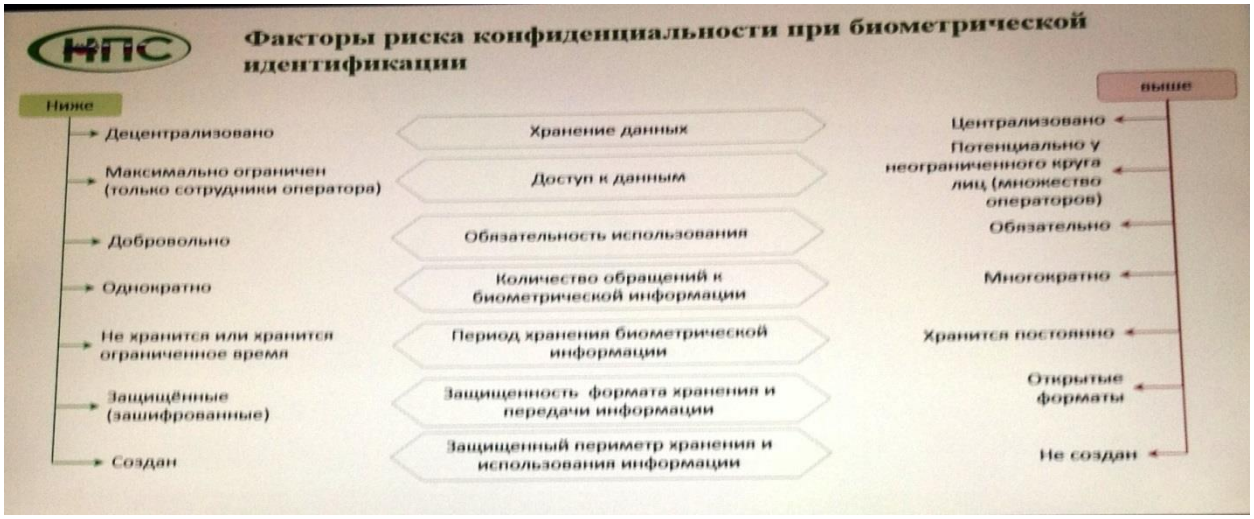


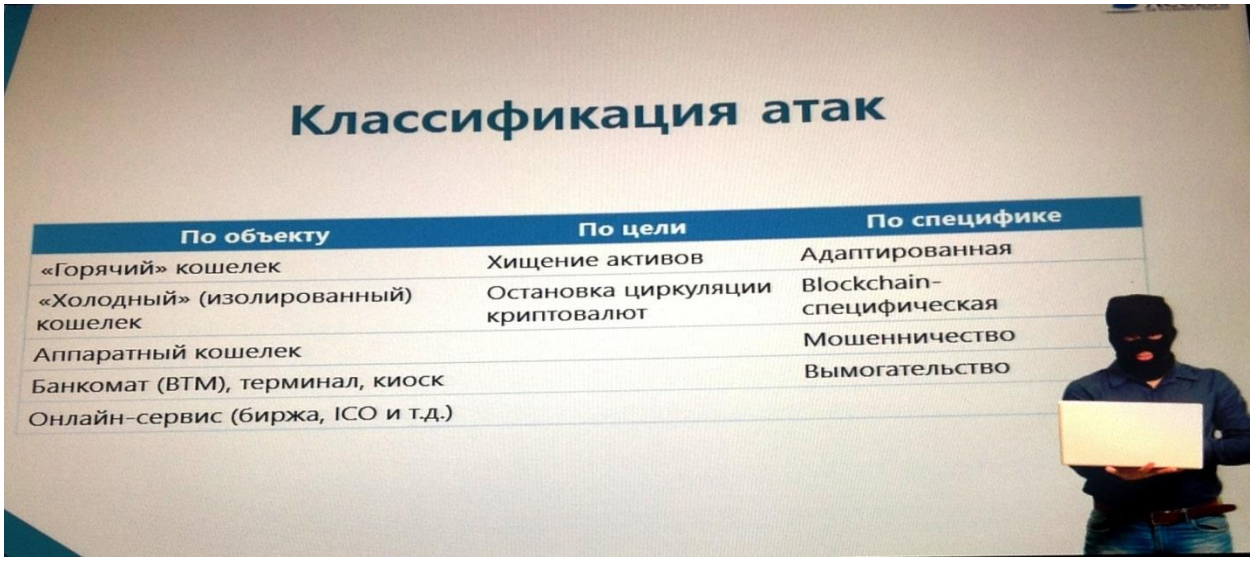




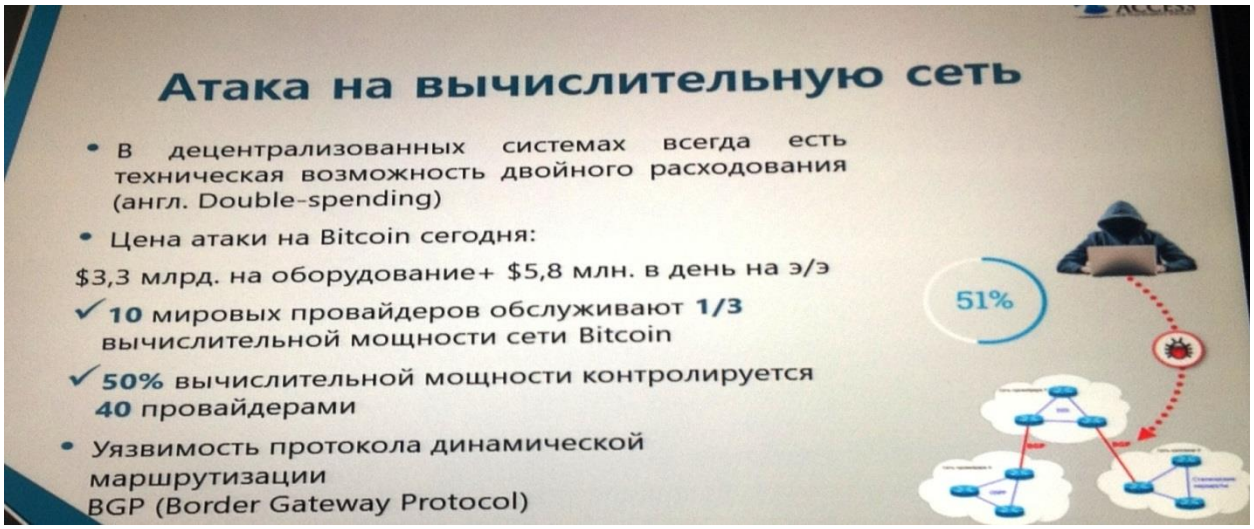

Текущее состояние защищенности Интернета вещей от киберугроз
2020
4 BILLION
54 TRILLION
25+ MILLION
25+ BILLION
50 TRILLION
THE INTERNET OF THINGS
По результатам исследований HP:
60% устройств обладают уязвимым веб-интерфейсом
70% наиболее часто используемых «умных» приборов, имеющих выход в сеть, уязвимы
80% устройств подвержены утечке информации в той или иной степени и когда-то «выдавали» личную информацию о своих владельцах
90% устройств собирают ту или иную персональную информацию о владельце без его ведома
Атаки не на «компьютерные» системы, а на «реальные» (кардиостимуляторы, бытовые устройства, автотранспорт и т.д.)


Трудности обеспечения безопасности КФС
Традиционные подходы не решают главную задачу
– Цель защиты КФС – обеспечение непрерывности процесса управления, а цель ИБ – обеспечение конфиденциальности, целостности, доступности данных
Непродуманность КФС с точки зрения безопасности
– Возможность идентификации киберфизических систем и ПО в локальных и глобальных сетях
– применение в современных КФС устаревших аппаратных и программных средств общего назначения
– Слабые средства авторизации и аутентификации («вшитые» в ПО аутентификационные данные по умолчанию, ненадежные алгоритмы и т.д.)
– Отсутствие шифрования в промышленных транспортных протоколах (modbus, s7comm и др.)
– Слабые средства аудита и регистрации событий
Негибкая архитектура КФС и АСУ ТП
– Невозможность внесения существенных изменений в системы
– Отсутствие обновлений операционных систем и приложений или невозможность их применить
– Высокий риск автоблокировки системы при внедрении средств защиты
Человеческий фактор


НПС
Факторы риска конфиденциальности при биометрической идентификации
Ниже
выше
Децентрализовано
Централизовано
Максимально ограничен (только сотрудники оператора)
Потенциально у неограниченного круга лиц (множество операторов)
Добровольно
Обязательно
Однократно
Многократно
Не хранится или хранится ограниченное время
Хранится постоянно
Защищённые (зашифрованные)
Открытые форматы
Создан
Не создан
Хранение данных
Доступ к данным
Обязательность использования
Количество обращений к биометрической информации
Период хранения биометрической информации
Защищенность формата хранения и передачи информации
Защищенный периметр хранения и использования информации


Классификация атак
По объекту
По цели
По специфике
«Горячий» кошелек
Хищение активов
Адаптированная
«Холодный» (изолированный) кошелек
Остановка циркуляции криптовалют
Blockchain-специфическая
Аппаратный кошелек
Мошенничество
Банкомат (BTM), терминал, киоск
Вымогательство
Онлайн-сервис (биржа, ICO и т.д.)

Адаптированные под Blockchain атаки
Похищение Private Key с помощью троянов
Вирусы-вымогатели [Ransomware]
Взлом банкоматов [BTM]
Фишинг
Социальная инженерия
Мошенничество


Атака на вычислительную сеть
В децентрализованных системах всегда есть техническая возможность двойного расходования (англ. Double-spending)
Цена атаки на Bitcoin сегодня:
$3,3 млрд. на оборудование+ $5,8 млн. в день на э/э
10 мировых провайдеров обслуживают 1/3 вычислительной мощности сети Bitcoin
50% вычислительной мощности контролируется 40 провайдерами
Уязвимость протокола динамической маршрутизации BGP (Border Gateway Protocol)
51%

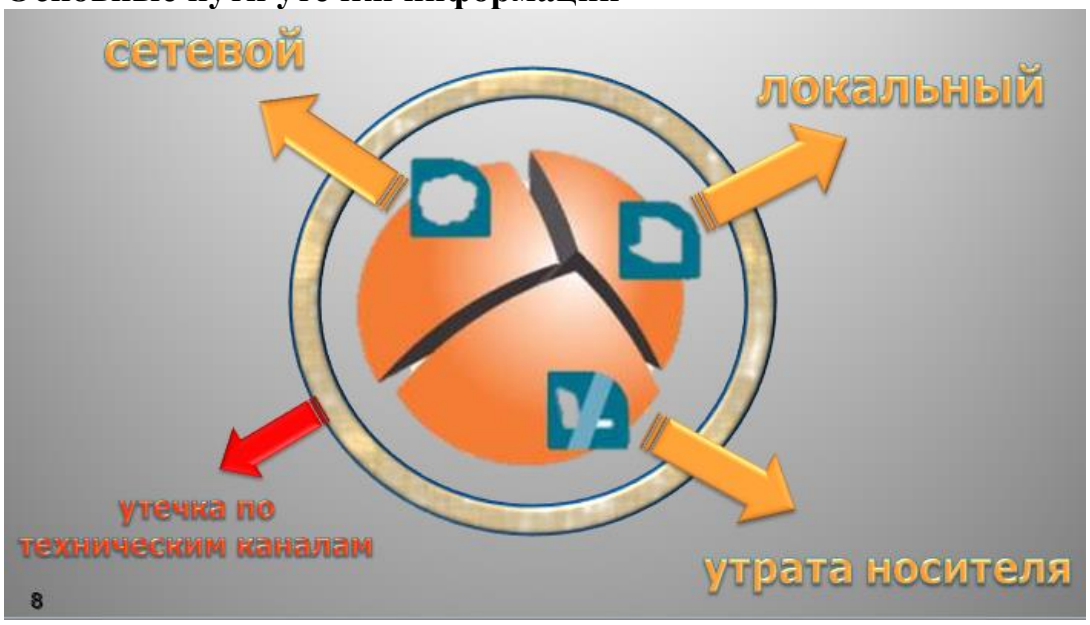
Угрозы безопасности информации (согласно Концепции ИБ ФНС)

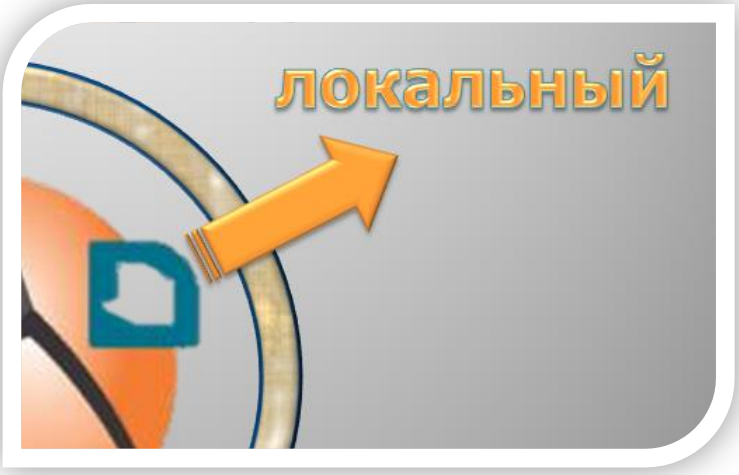
- **угрозы нарушения конфиденциальности**
- **угрозы нарушения целостности информации**
- **угрозы нарушения доступности информации**

Утечка конфиденциальной информации

бесконтрольный выход конфиденциальной информации за пределы ИС или круга лиц, которым она была доверена по службе или стала известна в процессе работы

Основные пути утечки информации

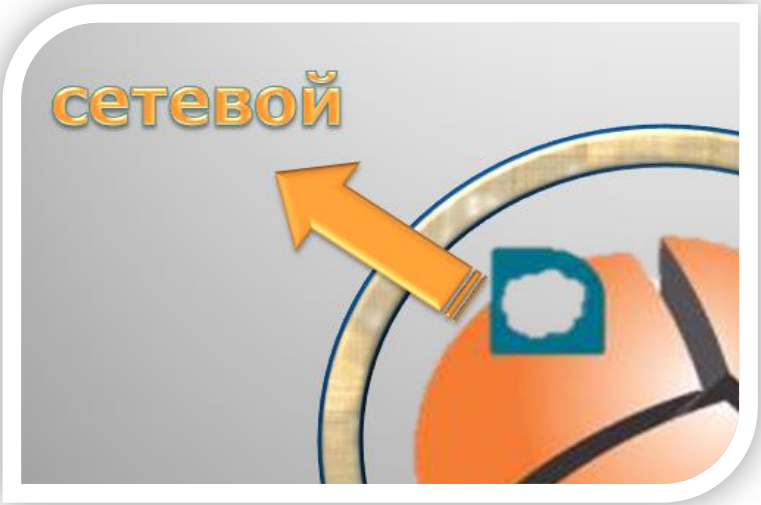




Копирование данных:

- **дискеты**

- **USB-накопители**
- **CD/DVD-накопители**
- **локальная печать («твердые копии»)**



- **почта (e-mail, web mail)**
- **передача файлов (локальная сеть, ftp, Wi-Fi)**
- **сетевая печать**
- **удаленное администрирование**

- **кража носителя**
- **потеря носителя**
  - **локальный носитель (дискета, USB-накопитель, CD/DVD-накопитель)**
  - **ноутбук**
  - **смартфон, КПК**

- **виброакустический**
- **побочные электромагнитные излучения**
- **активный перехват по проводным линиям**
- **радио и видеозакладки**
- **иные**

УДК 614.8.01

М.И. Фалеев, Г.С. Черных

Угрозы национальной безопасности государства в информационной сфере и задачи МЧС России в этой области деятельности

Аннотация
В статье рассмотрены угрозы национальной безопасности государства в информационной сфере и задачи МЧС России в этой области деятельности. Освещены наиболее уязвимые объекты МЧС России в сфере обеспечения информационной безопасности. Материалы статьи могут использоваться при планировании и выработке мер по снижению негативного психологического воздействия на население и личный состав формирований гражданской обороны (далее — ГО) в зонах чрезвычайных ситуаций (далее — ЧС), а также внедряться в практику спасательных сил МЧС России при решении организационных и других вопросов обеспечения информационной безопасности.
Ключевые слова: информационная безопасность; киберпространство; защита; информатизация; компьютеризация; информационные ресурсы; противоборство; сеть; управление.

Содержание

Введение
- Основные информационные угрозы России, обусловленные формированием единого киберпространства и пути их локализации
- Основные угрозы информационной безопасности государства в различных сферах общественной жизни и меры противодействия им
- Задачи МЧС России по обеспечению информационной безопасности государства Заключение

Литература

Введение

Стремительные темпы развития компьютеризации и информатизации общества неизбежно ведут к созданию единого мирового информационного

пространства, в котором будут аккумулированы все средства сбора, накопления, обработки, хранения и обмена информацией между отдельными людьми, организациями и государствами. В XXI веке основу мирового информационного пространства составят национальные информаци- онно-управляющие инфраструктуры развитых государств, таких как США, Китая, стран Западной Европы и Японии. При этом уже сейчас создаются предпосылки значительного роста политического, экономического и военного превосходства развитых индустриальных стран за счет их лидирующей роли в компьютеризации и информатизации.

Потенциально возрастающие технологические возможности информатизации находят все большее применение в таких жизненно важных сферах деятельности общества как телекоммуникация, энергетика, транспорт, системы хранения газа и нефти, финансовая и банковская системы, водоснабжение, оборона и национальная безопасность, структуры обеспечения устойчивой работы министерств и ведомств и т.д.

Кроме того, неотъемлемой частью инфраструктуры государств становятся сеть Интернет, глобальные и локальные вычислительные сети, компьютеры, факсы и факс-модемы, волоконно-оптическая связь, электронная почта, разветвленная сеть радио- и спутниковой связи. Это значительно увеличивает объемы и скорость информационных обменов на транснациональном уровне.

МЧС России в последние годы все чаще приходится сталкиваться с чрезвычайными ситуациями, характеризующимися их быстрым развитием, комплексностью и трудно прогнозируемыми последствиями. В таких условиях развитие технологий и разработка современных технических средств, осуществляющих прием, обработку, передачу информации об угрозе возникновения или о возникновении ЧС и их защита от враждебного проникновения является актуальной задачей.

Наиболее уязвимыми объектами обеспечения информационной безопасности России в условиях ЧС являются: система принятия решений по оперативным действиям (реакциям), связанным с развитием таких ситуаций и ходом ликвидации их последствий; система сбора и обработки информации о возможном возникновении ЧС; информационные каналы в ходе выполнения задач гуманитарной помощи за рубежом.

В соответствии с Указом Президента Российской Федерации от 13 ноября 2012 г. № 1522 МЧС России развернуты работы по созданию до 1 января 2014 г. комплексной системы экстренного оповещения населения об угрозе возникновения или о возникновении ЧС (КСЭОН). Необходимо подчеркнуть, что функционирование данной системы будет проходить в условиях информационного противоборства и нейтрализация негативного воздействия на ее структурные элементы, что является приоритетной задачей для МЧС России. В интересах реализации поставленных задач разработана Концепция создания КСЭОН, которая также призвана обеспечить безопасность государства в информационной сфере деятельности МЧС России. Рассмотрению информационных угроз национальной безопасности государства и задач МЧС России в данной области посвящен предлагаемый аналитический материал.

• Основные информационные угрозы России, обусловленные формированием единого киберпространства и пути их локализации

Информатизация всех сфер жизнедеятельности Российского государства, обусловленная лавинообразным развитием новых информационных и телекоммуникационных технологий способствовала тому, что информация и IT-системы[1] приобрели огромную значимость. Решение задач обеспечения национальной, военной, экономической безопасности может быть осуществлено только при условии применения новых информационных технологий (НИТ) в различных предметных областях, формирования системы комплексной безопасности информационных систем государственного и военного управления.

Объем информации, обрабатываемый (добываемый, хранимый, передаваемый и т.д.) с помощью глобальных информационных сетей, значительно (по разным оценкам в 2,5 — 5 раз) превосходит объем информации, обрабатываемый традиционными способами (бумажные носители, видео-, аудиоинформация и др.).

Процессы интеграции России в мировую экономическую систему с развитием информационных систем и технологий формируют тайную и скрытую для государства угрозу. Эта угроза обусловлена стремлением различных государственных и общественных институтов наиболее развитых государств мира (США, страны-члены блока НАТО,
Китай, Япония) получить доступ к российской информационной сфере (в основном конфиденциальной) с целью обобщения (анализа) информации, её трансформации (модификации), хищения (искажения) и т.п.

Имеющиеся уже в настоящее время угрозы еще более возрастают по мере расширения прав доступа населения в глобальную информационную сеть Интернет. Это связано со стремлением определенных пользователей к получению дополнительных знаний (сведений), касающихся жизнедеятельности государства, функционирования органов государственного и военного управления, деятельности лиц, принимающих решения и членов их семей.

Внедрение новых информационных технологий приводит к существенному росту качества управления государством, Вооруженными Силами, МЧС России и другими государственными институтами, а также порождает новый тип деяний[2], в которых информация становится объектом противоправного посягательства, а сами информационные технологии — орудием такого рода посягательств.

Анализ деятельности военно-политического ру-

ководства наиболее развитых государств мира в области разработки и реализации новых информационных технологий в сфере управления вооруженными силами показывает, что новая сфера их применения — киберпространство. Оно в отличие от «традиционных» сфер не имеет четко обозначенных географических границ, но является международным.

Нормативная правовая и научная база формирования киберпространства, определения его структуры, порядка функционирования в настоящий момент отсутствует. Практически все государства мира вынуждены «терпеть» экспансию США в Интернет-ресурсах, которые являются глобальным провайдером в сфере информационных услуг. Сам по себе Интернет, являясь глобальной информационной системой, представляет собой только лишь здает угрозу оказания программно-аппаратных воздействий посредством, как удаленного (дистанционного), так и непосредственного доступа в информационную сеть. Уровень развития технических средств (связи, передачи данных) не гарантирует полной безопасности информационной системы. Он формирует еще одну угрозу по оказанию деструктивных воздействий на информационные ресурсы государства и его различные институты, в том числе и на силовые структуры государства.

Своевременное обнаружение и выявление попыток доступа в информационную сеть в современных условиях технически трудно реализуемы. Уровень развития средств и технологий не позволяет обеспечить контроль несанкционированного доступа и безопасности информационных ресурсов.

Военно-политическое руководство США заботилось о повышении надежности и эффективности функционирования компьютерных сетей государственного и военного назначения. Не умаляя значимости ядерных и обычных (в том числе высокоточных) вооружений, военные эксперты США отмечают, что в современных условиях особую значимость приобретают «кибернетические аспекты». США, достигнув технологического превосходства практически во всех областях, тем не менее, подвержены серьезным угрозам, прежде всего, в киберпространстве.

Возможность использования мобильных телефонов, смартфонов, приборов глобальной навигации и др. устройств различными организациями и персоналиями для проникновения в информационные сети государственного и военного управления наносит существенный ущерб информационной безопасности государства. Этот ущерб заключается в нарушении обмена информацией, срыве процессов принятия решений, планирования и управления. Ведущие специалисты в области IT-технологий наиболее развитых государств мира отмечают тот факт, что «государство, контролирующее киберпространство будет контролировать войну и мир»[3].

Возникла необходимость перехода от традиционного оборонительного ориентирования в киберпространстве к наступательному. В армии США разработана «наступательная стратегия для нанесения ударов по киберсредствам противника»[4]. Реализация такой стратегии, по мнению военного руководства США, позволит уйти от возможного коллапса. Ему может быть подвержено государство и его ресурсы в результате «обороны в киберпространстве».

составляющую киберпространства.

Киберпространство формируется за счет объединения в единую глобальную информационную систему локальных, локально-распределенных, распределенных вычислительных сетей и выделенных пользовательских автоматизированных рабочих мест. В этой связи серьезную угрозу национальной, военной и информационной безопасности государства представляют формируемые на основе доступа в Интернет объединения в относительно малые группы пользователей (конфедерации хакеров), обладающих достаточной квалификацией.

Использование в киберпространстве общего для всех пользователей программного обеспечения, общих алгоритмов функционирования и применения новых информационных технологий создает в киберпространстве к наступательному.

В 2007 г. в армии США создано командование кибернетических операций Военно-Воздушных Сил (ВВС) с задачей минимизации ущерба в киберсреде и «...использования глобальной кибернетической мощи во всех видах конфликтов в качестве обеспечивающей компоненты объединенных группировок» (Министр ВВС США М.у. Уинни, 2007 г.).

Наращивание «кибернетической мощи» связано с тем, что в отличие от дорогостоящих систем оружия (системы высокоточного, ядерного оружия, другое современное вооружение) средства, применяемые в киберпространстве, позволяют «.создать очень дешево хаос издалека». Учитывая, что киберпространство все более охватывает электромагнитный спектр, можно ожидать, что деструктивному воздействию могут быть подвержены не только компьютерные системы, но и люди.

Создание киберпространства является необходимым условием формирования единого информационно-боевого пространства, обеспечивающего доминирующее положение в информационной сфере за счет:

оптимизации информационных потоков, обеспечивающих эффективное применение войск (сил), устойчивое и оперативное взаимодействие с системой государственного и военного управления всего государства;

направленного воздействия на информационные системы и потоки противника с целью разрушения (поражения, уничтожения, модификации) его информационных систем и ресурсов, дезорганизации вооруженных сил, системы государственного и военного управления.

Основными целями информационных действий в киберпространстве могут быть: контроль информационной сферы; использование киберпространства для интеграции военных действий в других

сферах (суша, вода, воздух, космос); обеспечение адекватности противодействий и безопасности сетей в информационной сфере; использование киберпространства для обеспечения разведывательных действий и операций влияния.

Американские специалисты отмечают, что основные положения национальной военной стратегии США не адекватны тем угрозам, которые возникают в ходе стратегического информационного противоборства (далее — ИП). В связи с этим они высказали необходимость расположения центра координации работ по противодействию угрозам в информационной сфере в непосредственной близости от президента.

Этим обеспечивается требуемый уровень координации деятельности всех министерств и ведомств: оценка уязвимости ключевых элементов национальной информационной инфраструктуры; обеспечение главенствующей роли государства в координации работ по противодействию угрозам в информационной сфере; внесение корректив в национальную стратегию безопасности и национальную военную стратегию и в ИП.

В условиях определенной трансформации взглядов на проблему ведения ИП изменяются и задачи по

достижению поставленной цели. По своему содержанию ИП разделяют на два поколения. Так, для информационного противоборства первого поколения характерна постановка следующих задач:
огневое подавление (в военное время) элементов инфраструктуры государственного и военного управления;

ведение радиоэлектронной борьбы; получение разведывательной информации путем перехвата и расшифровки информационных потоков, передаваемых по каналам связи, а также по побочным излучениям;

осуществление несанкционированного доступа к информационным ресурсам с последующим их искажением или хищением;

формирование и массовое распространение по информационным каналам противника или глобальным сетям дезинформации для воздействия на оценки, намерения лиц, принимающих решения;

получение интересующей информации путем перехвата открытых источников информации.

Информационное противоборство второго поколения включает несколько иной перечень задач:
создание атмосферы бездуховности и безнравственности, негативного отношения к культурному наследию противника;

манипулирование общественным сознанием и политической ориентацией социальных групп населения страны с целью создания политической напряженности и хаоса;

дестабилизация политических отношений между партиями, объединениями и движениями с целью провокации конфликтов, разжигание недоверия, подозрительности, обострения политической борьбы, провоцирование репрессий против оппозиции и даже развертывание гражданской войны;

снижение уровня информационного обеспечения органов власти и управления, инспирация ошибочных управленческих решений;

дезинформация населения о работе государственных органов, подрыв их авторитета, дискредитация органов управления;

провоцирование социальных, политических, национальных и религиозных столкновений;

инициирование забастовок, массовых беспорядков и других акций экономического протеста;

затруднение принятия органами управления необходимых решений;

подрыв международного авторитета государства, его сотрудничества с другими странами;

нанесение ущерба жизненно важным интересам государства в политической, экономической, оборонной и других сферах.

Непосредственную угрозу информационной безопасности России представляет создание в армиях наиболее развитых стран мира (США, Китай, Франция, Великобритания, Германия) подразделений информационных операций (сетевой борьбы, сетевых операций). Они проводят исследования, разрабатывают технологии ИП, обнаруживают и противодействуют попыткам проникновения в свои сетевые и в информационные ресурсы вооруженных сил и государства.

В Вооруженных силах США создано объединенное кибернетическое командование (США Cyber Command). Оно подчинено Стратегическому командованию Соединенных Штатов и предназначено решать многочисленные задачи по отражению атак на информационные сети США как враждебных государств, так и отдельных организаций или хакеров.

Создание кибернетического командования обусловило разработку новой стратегии обеспечения безопасности информационных ресурсов Пентагона, в рамках которой в функции формируемого командования войдет не только защита военных компьютерных сетей США, но и проведение атак на информационные сети вероятных противников Америки.

Создание основных технических предпосылок для формирования киберпространства в полном объеме планируется к 2015 году, а полная функциональная готовность — к 2020 году. Ежегодные расходы США на эти цели могут составить до 6 млрд долл., а общие расходы до 2020 года могут превысить 80 млрд долл.

Создание в армиях государств структур, предназначенных для защиты информационных систем и воздействия на информационные системы противника, позволит решать задачи блокирования «национальной воли», достижения «малокровного и молниеносного паралича системы государственного и военного управления», превращения вооруженной борьбы в односторонний процесс и др.

По взглядам зарубежных военных экспертов с созданием «единого информационного пространства» (единого киберпространства) наступит новая эра в вооруженной борьбе — эра «явного (абсолютного) информационного и боевого превосходства».

В современных военных операциях предусматривается:

до начала агрессии (мирное время, угрожаемый период) — ведение сторонами активного информационного противоборства. Оно включает в себя: мощное информационно-психологическое воздействие на инфраструктуру государства и мировое сообщество; информационно-техническое воздействий на систему государственного и военного управления, на средства телекоммуникации и связи, объекты разведки, РЭБ и др.;

до начала военных действий — проведение подрывных мероприятий со стороны внедренной агентуры, диверсионно-разведывательных и незаконных (иррегулярных) формирований, различных сетевых структур и т.п.;

до начала полномасштабных военных действий (как правило, за несколько часов) — поражение (разгром, уничтожение) орбитальной группировки космических аппаратов и захват объектов ядерного оружейного комплекса противника специально подготовленными силами.

В целом все киберугрозы следует разделить на три группы: хакерские, криминальные и киберугрозы со стороны спецслужб. Это требует создания технологий, обеспечивающих эффективное противодействие кибератакам. Военно-политическое руководство США определяет киберсферу как единственную область противоборства, где у США имеются равные противники (Китай и Россия).

Рост количества и масштабов электронных угроз, их постоянная трансформация требует создания в России единого Федерального центра защиты информационной сферы. На него следует возложить разработку нормативной правовой базы, идеологии обеспечения информационной безопасности России, интеграции усилий государственных и коммерческих организаций по разработке и внедрению единых стандартов обеспечения информационной безопасности и др.

В настоящее время зарождается направление военных и политических технологий, строящихся на способах манипуляции и искажения информации в политических системах стран — потенциальных противников. Массовое распространение Интернета позволило получить универсальный и уникальный вектор воздействия на психику индивида. Интернет стал недостающим звеном цепи, способным соединить воедино информационную и психологическую войны.

Сферы применения и цели информационного оружия приведены в табл. 1.

В последние годы в министерстве обороны США активизируются работы по созданию информационно-психологического оружия как одного из компонентов ведения информационной войны. Эксперты определяют это оружие как совокупность средств и методов, позволяющих: похищать, искажать или уничтожать информацию; ограничивать или прекращать доступ к ней законных пользователей; нарушать работу или выводить из строя телекоммуникационные сети и компьютерные системы, используемые в обеспечении жизнедеятельности общества и государства.

Основные виды информационно-психологического оружия, применимые к использованию в глобальных кибернетических сетях гражданского назначения и открытого доступа приведены в табл. 2.

Анализ опыта локальных войн, вооруженных конфликтов и контртеррористических операций современности показывает, что конфликтующие стороны в качестве одного из основных инструментов воздействия на противника все чаще используют методы информационно-психологического оружия.

В ходе войны в Ираке вооруженные силы коалиции применили против иракских радиоэлектронных средств электромагнитную бомбу. Это устройство преобразует химическую энергию взрывчатого вещества в электромагнитный импульс высокой мощности (до 10 Гигаватт-час), что соответствует мощности крупной ГРЭС. При этом поражаются компоненты радиоэлектронной техники в радиусе более 250 метров и тем самым выводятся из строя системы связи, информатики и управления.

Психологическое воздействие опасно тем, что в отличие от первых двух стратегий использования информационного оружия, его гораздо труднее обнаружить на ранних стадиях применения, не говоря уже о невозможности его выявления программно-аппаратными средствами.

Неэквивалентный информационный обмен между глобальным центром и глобальной периферией, как указывают российские исследователи, таит в себе угрозу не только утраты национальной культуры информационного реципиента, но и потерю чувства реальности. Так в высших сферах военного руководства США господствует убежденность в том, что: «... главной чертой вооруженной борьбы в XXI веке будет перенос акцента в сферу информационного противоборства и достижение «информационного господства» станет обязательным условием победы над любым противником».

Таблица 1

Сферы применения и цели информационного оружия

Военная сфера	**Политическая сфера**
Объект атаки	
Системы управления войсками, средства ПВО, связь, противоракетная оборона, компьютерные комплексы координации работы войск и принятия военных решений	Национальное самосознание, политические настроения населения, моральное состояние войск, ценностные и мировоззренческие установки правящей элиты
Способы	
Физические средства подавления и разрушения информационных объектов противника	Искажение информации в СМИ, слухи, дезинформация, воздействие на психику человека
Назначение	
Применяется для достижения быстрого успеха в тактических военных операциях	Применяется для достижения успеха в долгосрочном военно-политическом противостоянии, в том числе и вне фазы ведения боевых действий
Достигаемый эффект	
Потерявшие управление войска противника снижают степень эффективности сопротивления. Яркими примерами являются военные кампании против Ирака и Югославии	Общее снижение обороноспособности и политической устойчивости государства противника. В случае особого успеха происходит свержение неугодного правительства или распад враждебной страны

Стратегия нападения		
Системы дистанционного уничтожения или искажения информации в кибернетических системах	Системы хищения информации и несанкционированного доступа на удаленный компьютер	Системы комплексного воздействия на психику пользователя Интернета
Вид оружия		
Компьютерные вирусы общего и специализированного назначения, адаптированные к работе в конкретных электронных компьютерных сетях по конкретным протоколам (программы, проникающие извне и разрушающие систему деструктивными действиями). *Логические бомбы* — недокументированный аппаратный набор, (микросхема, чип, и т.д.) тайно внедряемый в компьютер на этапе заводской сборки в расчете на то, что данное «оргоборудование» попадет в соответствующие ведомства «интересующей» страны. При активизации парализует работу компьютера и, соответственно, нарушает функционирование системы	*Электронные шпионы* общего и специализированного назначения, адаптированные к работе в конкретных электронных компьютерных сетях по конкретным протоколам (программы, проникающие извне и производящие незаметный для пользователя съем служебной системной и непосредственной приватной информации пользователя)	*Мультимедийные сайты,* представленные в виде информационно-развлекательных или аналитических страниц с «горячей», «сенсационной» и т.д. информацией, составленные с учетом законов особенностей восприятия человека и психологии виртуальных коммуникаций

Значительно упростилась система управления боевыми отрядами, процедура адресного рекрутинга боевиков и политических адептов. По спутниковой беспроводной Интернет-связи террористы размещают информацию о потребности в боевиках для проведения той или иной акции, проводят переговоры со всеми желающими, фильтруют информацию спецслужб, производят закупки оружия, денежные переводы за оплату услуг боевиков и контролируют результаты проведения заказанной операции.

При этом руководящий штаб экстремистов сам находится в состоянии неуязвимости для служб безопасности той страны, против которой готовилась диверсия. Единственным ответом, как показал опыт США, может стать лишь широкомасштабная военная экспансия на территорию страны, где расположен координирующий центр террористов.

С развитием электронных сетей террористы получили качественно новую возможность для пропаганды своих идей, для показательной полемики с официальными государственными структурами, для дискредитации и дезавуирования заявлений официальных властей.

Компьютеризация (автоматизация) административно-управленческих процессов существенно повышает уязвимость функционирования системы путем использования чрезвычайно дешевых и доступных методов информационно-компьютерных диверсий. Пока под удар попадают как раз наиболее развитые страны, с высокой степенью развития открытых электронных информационных систем — более 50 % пользователей Интернета проживают в США и Канаде.

В российских сетевых СМИ был оглашен факт функционирования в Сан-Франциско русскоязычного сервера. С него предлагались к продаже российские конфиденциальные информационные продукты служебного пользования. Это были служебные базы: «Лабиринт» (база данных о российских политиках и их биографиях), «Лунар» (телефоны и справочная информация о руководящем составе МВД, налоговой полиции, правительства, прокуратуры, Газпрома и пр.), «БТИ» (собственники жилья в Москве), «ГИБДД» (полные данные по автовладельцам Москвы) и другие [Inroad Hi-Tech Review].

В мировом киберсообществе уже сложились интернациональные кланы хакеров, преследующих в сети политические или околополитические цели. Развитие информационных технологий, повышающих информационную и идеологическую уязвимость политической системы, вызывает ответную реакцию государств и транснациональных структур. Она выражается в форме усиления контроля всеми доступными методами — от юридических до аппаратно-программных.

В настоящее время постепенно выстраивается своеобразная система управления сознанием и поведением конкретного индивида, социальных страт и наций. Это формирует опасный фундамент развития неототалитарных политических процессов в ближайшие десятилетия.

Все более очевидной (а значит — потенциально целенаправленно управляемой) становится тенденция роста роли и влияния мнения неформальных лидеров, активно общающихся на информационных сетевых полях. При этом они зачастую искажают факты, делают неверные выводы и выносят предложения, носящие откровенно провокационный характер. Мнение официальных лидеров, квалифицированных экспертов не воспринимается информационным сообществом, чаще всего под «ярлыком» ангажированности.

Особую опасность такого рода информационная активность представляет в чрезвычайных ситуациях. В ходе ликвидации последствий наводнения в г. Крымске (2011 г.) целенаправленно распространялись, в основном через Интернет, слухи о предстоящих спусках воды из вышерасположен-

ных водохранилищ, что вызывало панические настроения у населения. При вспышке инфекционного менингита в г. Ростове на Дону (2013 г.) через компьютерную сеть и SMS-собщения в мобильной телефонной сети жители оповещались о предстоящей дезинфекционной обработке территории авиацией, что не соответствовало действительности и дезориентировало граждан.

Такого рода инциденты могут в будущем носить системный характер. Поэтому в технологии ликвидации последствий ЧС следует предусматривать структуру информационной поддержки, в которую должны вовлекаться местные специалисты и компетентные неформальные лидеры Интернет-общения.

Серьезную хакерскую атаку с территории третьей страны удалось преодолеть специалистам НЦУКС в 2000 г. при проведении российско-американских командно-штабных учений, отрабатывающих совместные действия информационно-управ- ляющих центров (Москва, Хабаровск и Гонолулу) при моделировании землетрясений и цунами в Тихом океане. Однако хакерские технологии с каждым годом совершенствуются, поэтому и меры противодействия им также должны систематически модернизироваться.

• Основные угрозы информационной безопасности государства в различных сферах общественной жизни и меры противодействия им

Доктрина информационной безопасности Российской Федерации развивает положения Концепции национальной безопасности Российской Федерации о том, что информационная безопасность России является одной из составляющих национальной безопасности. Она оказывает влияние на защищенность национальных интересов страны в таких сферах жизнедеятельности общества и государства как: экономика, внутренняя политика, наука и техника, духовная жизнь, общегосударственные информационные и телекоммуникационные системы, оборона, правоохранительная и судебная.

Угрозы информационной безопасности России и методы ее обеспечения являются общими для этих сфер. В каждой из них имеются свои особенности обеспечения информационной безопасности, связанные со спецификой объектов обеспечения безопасности, степенью их уязвимости в отношении таких угроз.

В каждой вышеперечисленных сфер жизнедеятельности общества и государства могут использоваться частные методы, способы и формы обеспечения информационной безопасности, обусловленные спецификой факторов, влияющих на состояние информационной безопасности России.

В сфере экономики воздействию угроз информационной безопасности России наиболее подвержены следующие системы: государственная статистика; кредитно-финансовая; информационная и учетные автоматизированные системы обработки учетной информации подразделений федеральных органов исполнительной власти, обеспечивающих деятельность общества и государства в сфере экономики; бухгалтерского учета предприятий, учреждений и организаций независимо от формы собственности; сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации и информации о внешнеэкономической деятельности государства, а также предприятий, учреждений и организаций независимо от формы собственности.

Переход к рыночным отношениям в экономике вызвал появление на внутреннем российском рынке товаров и услуг множества отечественных и зарубежных коммерческих структур — производителей и потребителей информации, средств информатизации и защиты информации. Бесконтрольная деятельность этих структур по созданию и защите систем сбора, по обработке, хранению и передаче статистической, финансовой, биржевой, налоговой, таможенной информации создает реальную угрозу безопасности России в экономической сфере.

Аналогичные угрозы возникают при бесконтрольном привлечении иностранных фирм к созданию подобных систем, поскольку при этом складываются благоприятные условия для несанкционированного доступа к конфиденциальной экономической информации и для контроля процесса ее передачи и обработки со стороны иностранных спецслужб.

Слабое технологическое состояние предприятий национальных отраслей промышленности, разрабатывающих и производящих средства информатизации, телекоммуникации, связи и защиты информации, приводит к широкому использованию соответствующих импортных средств. Это создает угрозу возникновения технологической зависимости России от иностранных государств.

Угрозу для нормального функционирования экономики представляют компьютерные преступления, связанные с проникновением криминальных элементов в компьютерные системы и сети банков и иных кредитных организаций.

Несовершенство нормативной правовой базы, определяющей ответственность хозяйствующих субъектов за недостоверность или сокрытие сведений об их коммерческой деятельности, о потребительских свойствах производимых ими товаров и услуг о результатах их хозяйственной деятельности, об инвестициях и тому подобном, препятствует нормальному функционированию хозяйствующих субъектов. В то же время существенный экономический ущерб хозяйствующим субъектам может быть нанесен вследствие разглашения информации, содержащей коммерческую тайну.

В системах сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной

информации наиболее опасно противоправное копирование информации и ее искажение вследствие преднамеренных или случайных нарушений технологии работы с информацией, несанкционированного доступа к ней.

Основными мерами по обеспечению информационной безопасности государства в сфере экономики являются:

организация и осуществление государственного контроля за созданием, развитием и защитой систем и средств сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации;

формирование и развитие системы государственной статистической отчетности в целях обеспечения достоверности, полноты и защищенности информации;

разработка национальных сертифицированных средств защиты информации и внедрение их в системы и средства сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации;

разработка и внедрение национальных защищенных систем электронных платежей на базе интеллектуальных карт, систем электронных денег и электронной торговли, стандартизация этих систем, а также разработка нормативной правовой базы, регламентирующей их использование;

совершенствование нормативной правовой базы, регулирующей информационные отношения в сфере экономики;

совершенствование методов отбора и подготовки персонала для работы в системах сбора, обработки, хранения и передачи экономической информации.

Наиболее важными объектами обеспечения информационной безопасности России в сфере внутренней политики являются:

конституционные права и свободы человека и гражданина;

конституционный строй, национальное согласие, стабильность государственной власти, суверенитет и территориальная целостность Российской Федерации;

открытые информационные ресурсы федеральных органов исполнительной власти и средств массовой информации.

Наибольшую опасность в сфере внутренней политики представляют следующие угрозы информационной безопасности Российской Федерации: нарушение конституционных прав и свобод граждан, реализуемых в информационной сфере;

недостаточное правовое регулирование отношений в области прав различных политических сил на использование средств массовой информации для пропаганды своих идей;

распространение дезинформации о политике Российской Федерации, деятельности федеральных органов государственной власти, событиях, происходящих в стране и за рубежом;

деятельность деструктивных общественных объединений, направленная на насильственное изменение основ конституционного строя и нарушение целостности России, разжигание социальной, расовой, национальной и религиозной вражды.

Основными мероприятиями в области обеспечения информационной безопасности России в сфере внутренней политики являются:

создание системы противодействия монополизации отечественными и зарубежными структурами составляющих элементов информационной инфраструктуры, включая рынок информационных услуг и средств массовой информации;

активизация контрпропагандистской деятельности, направленной на предотвращение негативных последствий распространения дезинформации о внутренней политике России.

К наиболее важным объектам обеспечения информационной безопасности России в сфере внешней политики относятся:

информационные ресурсы представительств федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств России при международных организациях;

информационные ресурсы представительств федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации на территориях субъектов Российской Федерации;

информационные ресурсы российских предприятий, учреждений и организаций, подведомственных федеральным органам исполнительной власти, реализующим внешнюю политику Российской Федерации;

деятельность российских средств массовой информации по разъяснению зарубежной аудитории целей и основных направлений государственной политики Российской Федерации, ее мнения по социально значимым событиям российской и международной жизни.

Из внешних угроз информационной безопасности России в сфере внешней политики наибольшую опасность представляют:

информационное воздействие иностранных политических, экономических, военных и информационных структур на разработку и реализацию стратегии внешней политики Российской Федерации;

распространение за рубежом дезинформации о внешней политике Российской Федерации;

нарушение прав российских граждан и юридических лиц в информационной сфере за рубежом;

попытки несанкционированного доступа к информации и воздействия на информационные ресурсы, информационную инфраструктуру федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств России при международных организациях.

Из внутренних угроз информационной безопасности России в сфере внешней политики наибольшую опасность представляют:

нарушение установленного порядка сбора, обработки, хранения и передачи информации в федеральных органах исполнительной власти, реализующих внешнюю политику Российской Федерации, и на подведомственных им предприятиях, в учреждениях и организациях;

информационно-пропагандистская деятельность политических сил, общественных объединений, средств массовой информации и отдельных лиц, искажающая стратегию и тактику внешнеполитической деятельности Российской Федерации;

недостаточная информированность населения о внешнеполитической деятельности Российской Федерации.

Основными мероприятиями по обеспечению информационной безопасности России в сфере внешней политики являются:

разработка основных направлений государственной политики в области информационного обеспечения внешнеполитического курса Российской Федерации;

разработка и реализация комплекса мер по усилению информационной безопасности информационной инфраструктуры федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств России при международных организациях;

создание российским представительствам и организациям за рубежом условий для работы по нейтрализации распространяемой там дезинформации о внешней политике Российской Федерации;

совершенствование информационного обеспечения работы по противодействию нарушениям прав и свобод российских граждан и юридических лиц за рубежом;

совершенствование информационного обеспечения субъектов Российской Федерации по вопросам внешнеполитической деятельности, которые входят в их компетенцию.

Наиболее важными объектами обеспечения информационной безопасности России в области науки и техники являются:

результаты фундаментальных, поисковых и прикладных научных исследований, потенциально важные для научно-технического, технологического и социально-экономического развития страны, включая сведения, утрата которых может нанести ущерб национальным интересам и престижу Российской Федерации;

открытия, незапатентованные технологии, промышленные образцы, полезные модели и экспериментальное оборудование;

научно-технические кадры и система их подготовки;

системы управления сложными исследовательскими комплексами (ядерными реакторами, ускорителями элементарных частиц, плазменными генераторами и другими).

К числу основных внешних угроз информационной безопасности России в области науки и техники следует отнести:

стремление развитых иностранных государств получить противоправный доступ к научно-техническим ресурсам России для использования полученных российскими учеными результатов в собственных интересах;

создание льготных условий на российском рынке для иностранной научно-технической продукции и стремление развитых стран в то же время ограничить развитие научно-технического потенциала России (скупка акций передовых предприятий с их последующим перепрофилированием, сохранение экспортно-импортных ограничений и тому подобное);

политику иностранных государств, направленную на дальнейшее разрушение унаследованного от СССР единого научно-технического пространства государств — участников Содружества Независимых Государств за счет переориентации на западные страны их научно-технических связей, а также отдельных, наиболее перспективных научных коллективов;

активизацию деятельности иностранных государственных и коммерческих предприятий, учреждений и организаций в области промышленного шпионажа с привлечением к ней разведывательных и специальных служб.

К числу основных внутренних угроз информационной безопасности России в области науки и техники следует отнести:

сохраняющуюся непростую экономическую ситуацию в России, ведущую к снижению финанси-

рования научно-технической деятельности, падению престижа научно-технической сферы, утечке за рубеж идей и передовых разработок;

неспособность предприятий национальных отраслей электронной промышленности производить конкурентоспособную наукоемкую продукцию микроэлектроники, позволяющую обеспечить достаточный уровень технологической независимости России от зарубежных стран;

состояние патентной защиты результатов научно-технической деятельности российских ученых;

сложность реализации мероприятий по защите информации в научно-технических учреждениях и организациях, в частности, на акционированных предприятиях.

Важным направлением противодействия угрозам информационной безопасности России в области науки и техники является совершенствование законодательства Российской Федерации. Государство должно способствовать созданию системы оценки возможного ущерба от реализации угроз наиболее важным объектам обеспечения информационной безопасности России в области науки и техники.

Обеспечение информационной безопасности России в сфере духовной жизни общества имеет целью защиту конституционных прав и свобод человека и гражданина. Оно связано с формированием и развитием личности, со свободой массового информирования, с использованием культурного, духовно-нравственного наследия, исторических традиций и норм общественной жизни, с сохранением культурного достояния всех народов России. Оно тесно связано с реализацией конституционных ограничений прав и свобод человека и гражданина в интересах сохранения и укрепления нравственных ценностей общества, традиций патриотизма и гуманизма, здоровья граждан, культурного и научного потенциала государства, обеспечения обороноспособности и безопасности государства.

К числу основных объектов обеспечения информационной безопасности России в сфере духовной жизни общества относятся:

достоинство личности, свобода совести, право выбора, право вероисповедания, свобода убеждений, свобода мысли и слова (за исключением пропаганды или агитации, возбуждающих социальную, расовую, национальную или религиозную ненависть и вражду), а также свобода литературного, художественного, научного, технического и других видов творчества;

свобода массовой информации; неприкосновенность частной жизни, личной и семейной тайны;

русский язык как фактор духовного единения народов многонациональной России, язык межгосударственного общения народов;

устные традиции и формы выражения, включая язык в качестве носителя нематериального культурного наследия народов России;

объекты интеллектуальной собственности. Наибольшую опасность в сфере духовной жизни общества представляют следующие угрозы информационной безопасности Российской Федерации: деформация системы массового информирования как за счет монополизации средств массовой информации, так и за счет неконтролируемого расширения сектора зарубежных средств массовой информации в отечественном информационном пространстве;

ухудшение состояния и постепенный упадок объектов российского культурного наследия, включая архивы, музейные фонды, библиотеки, памятники архитектуры;

нарушение общественной стабильности, нанесение вреда здоровью и жизни граждан вследствие деятельности религиозных объединений, проповедующих религиозный фундаментализм, а также тоталитарных религиозных сект;

использование зарубежными специальными службами средств массовой информации, действующих на территории России, для нанесения ущерба обороноспособности страны и безопасности государства, распространения дезинформации;

неспособность современного гражданского общества обеспечить формирование и поддержание в обществе нравственных ценностей, патриотизма и гражданской ответственности за судьбу страны.

Основными направлениями обеспечения информационной безопасности России в сфере духовной жизни общества являются:

развитие в России институтов гражданского общества;

создание социально-экономических условий для осуществления творческой деятельности и функционирования учреждений культуры;

выработка цивилизованных форм и способов общественного контроля формирования в обществе духовных ценностей, отвечающих национальным интересам страны, за воспитание патриотизма и гражданственности;

совершенствование законодательства России, регулирующего отношения в области конституционных ограничений прав и свобод гражданина;

государственная поддержка мероприятий по сохранению и возрождению культурного наследия народов и народностей Российской Федерации;

формирование правовых и организационных механизмов обеспечения конституционных прав и свобод граждан, повышения их правовой культуры;

противодействие сознательному или непреднамеренному нарушению конституционных прав и свобод в сфере духовной общества жизни;

разработка организационно-правовых механизмов доступа средств массовой информации и граждан к информации о деятельности федеральных органов государственной власти и общественных объединений;

разработка правовых и организационных механизмов недопущения противоправных информационно-психологических воздействий на массовое сознание общества, неконтролируемой коммерциализации культуры и науки;

введение запрета на использование эфирного времени в электронных средствах массовой информации для проката программ, пропагандирующих насилие и жестокость, антиобщественное поведение;

противодействие негативному влиянию иностранных религиозных организаций и миссионеров.

Основными объектами обеспечения информационной безопасности России в общегосударственных информационных телекоммуникационных системах являются:

информационные ресурсы, содержащие сведения, отнесенные к государственной тайне, и конфиденциальную информацию;

средства и системы информатизации, программные средства, автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации ограниченного доступа, их информативные физические поля;

технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается информация ограниченного доступа, а также сами помещения, предназначенные для обработки такой информации;

помещения, предназначенные для ведения закрытых переговоров, а также переговоров, в ходе которых оглашаются сведения ограниченного доступа.

Основными угрозами информационной безопасности России в общегосударственных информационных и телекоммуникационных системах являются:

деятельность специальных служб иностранных государств, преступных сообществ, организаций и групп, противозаконная деятельность отдельных лиц, направленная на получение несанкционированного доступа к информации и осуществление контроля за функционированием информационных и телекоммуникационных систем;

вынужденное использование при создании и развитии информационных и телекоммуникационных систем импортных программно-аппаратных средств;

нарушение установленного регламента сбора, обработки и передачи информации, преднамеренные действия и ошибки персонала информационных и телекоммуникационных систем, отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах;

использование не сертифицированных, не соответствующих требованиям безопасности средств и систем информатизации и связи, а также средств защиты информации и контроля их эффективности;

привлечение к работам по созданию, развитию и защите информационных и телекоммуникационных систем организаций и фирм, не имеющих государственных лицензий на осуществление этих видов деятельности.

Основными направлениями обеспечения информационной безопасности России в общегосударственных информационных и телекоммуникационных системах являются:

предотвращение перехвата информации из помещений специальных объектов, а также информации из каналов связи;

исключение несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации;

предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических средств, при обработке, хранении и передаче информации;

предотвращение умышленных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации;

обеспечение информационной безопасности при подключении общегосударственных информационных и телекоммуникационных систем к внешним информационным сетям, включая международные;

обеспечение безопасности конфиденциальной информации при взаимодействии информационных и телекоммуникационных систем различных классов защищенности;

выявление внедренных на объекты и в технические средства электронных устройств перехвата информации.

Основными организационно-техническими мероприятиями по защите информации в общегосударственных информационных и телекоммуникационных системах являются:

лицензирование деятельности организаций в области защиты информации;

аттестация объектов информатизации по выполнению требований обеспечения защиты информации при проведении работ, связанных с использованием сведений, составляющих государственную тайну;

сертификация средств защиты информации и контроля эффективности их использования, а также защищенности информации от утечки по техническим каналам систем и средств информатизации и связи;

введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;

создание и применение информационных и автоматизированных систем управления в защищенном исполнении.

К наиболее важным объектам обеспечения информационной безопасности в правоохранительной и судебной сферах относятся:

информационные ресурсы федеральных органов исполнительной власти, реализующих правоохранительные функции, судебных органов и их информационно-вычислительных центров, информационное, техническое, программное и нормативное обеспечение;

информационная инфраструктура (информационно-вычислительные сети, пункты управления, узлы и линии связи).

Внешними угрозами, представляющими наибольшую опасность для объектов обеспечения информационной безопасности в правоохранительной и судебной сферах, являются:

разведывательная деятельность специальных служб иностранных государств, международных преступных сообществ, организаций и групп;

деятельность иностранных государственных и частных коммерческих структур.

Внутренними угрозами, представляющими наибольшую опасность для указанных объектов, являются:

нарушение установленного регламента сбора, обработки, хранения и передачи служебной информации;

недостаточность законодательного и нормативного регулирования информационного обмена в правоохранительной и судебной сферах;

отсутствие единой методики сбора, обработки и хранения информации;

отказ технических средств и сбои программного обеспечения;

преднамеренные действия, а также ошибки персонала.

Применяются специфические методы и средства обеспечения информационной безопасности в правоохранительной и судебной сферах:

функционирование интегрированных банков данных на базе специализированных информационно-телекоммуникационных систем;

совершенствование профессиональной и специальной подготовки пользователей информационных систем.

• Задачи МЧС России по обеспечению информационной безопасности государства

В условиях информационного противоборства для МЧС России актуальной задачей является развитие технологий и разработка современных технических средств, осуществляющих прием, обработку, передачу и защиту информации об угрозе возникновения или о возникновении ЧС, особенно на потенциально опасных объектах, о правилах поведения и способах защиты населения в таких ситуациях.

На решение комплекса этих задач должна быть направлена работа действующих систем оповещения в составе РСЧС. Данное информационное пространство сферы деятельности МЧС России требует его всесторонней защиты в интересах безопасности государства.

В настоящее время в Российской Федерации созданы и функционируют региональные (в границах субъектов Российской Федерации), местные (в границах муниципальных образований) и локальные (объектовые) системы оповещения населения (в районах размещения потенциально опасных объектов).

Создается комплексная система экстренного оповещения населения (КСЭОН) об угрозе возникновения или о возникновении ЧС на территориях, подверженных воздействию опасных быстроразвивающихся природных явлений и техногенных процессов. Эта система должна быть защищена от несанкционированного проникновения в каналы сбора и передачи оперативной информации об обстановке в зоне ЧС.

Расширяется сфера применения общероссийской комплексной системы информирования и оповещения населения в местах массового пребывания людей (ОКСИОН) и системы защиты от угроз природного и техногенного характера, информирования и оповещения населения на транспорте (СЗИОНТ). Они предназначены для информирования и оповещения населения в местах массового

пребывания и на объектах транспортной инфраструктуры, функционирование которых предусматривается также в условиях информационного противоборства.

Условия быстро меняющихся рисков ЧС, развитие телекоммуникационных технологий, урбанизация населения требуют пересмотра подходов к дальнейшему развитию систем информирования и оповещения. Специальные системы централизованного оповещения (СЦО) должны быть обеспечены современными средствами защиты от несанкционированного проникновения в каналы сбора и передачи данных оперативной обстановки в зоне ЧС.

Повышение оперативности систем оповещения и информирования населения об угрозе возникновения или факте возникновения ЧС может быть достигнуто лишь путем автоматизации процессов и минимизации влияния человеческого фактора в них.

Наиболее уязвимыми объектами, с точки зрения, обеспечения информационной безопасности России в условиях ЧС являются система принятия решений по оперативным действиям (реакциям), связанным с развитием таких ситуаций и ходом ликвидации их последствий, а также система сбора и обработки информации о возможном возникновении ЧС.

Данные о потенциально опасных объектах особенно радиационного, химического, биологического (РХБ) характера могут быть использованы противником (деструктивными элементами) в интересах информационного противоборства путем распространения искаженных (ложных) сведений об РХБ и в целом экологической обстановке в определенном районе страны. Следствием этого может наступить дестабилизация обстановки и социальная напряженность среди населения.

Таблица 3

Информационная безопасное: в сфере гражданской обороны

Информационные угрозы и объекты воздействия в сфере ГО в условиях ЧС и меры обеспечения ее безопасности приведены в табл. 3.

Особое значение для функционирования указанных объектов имеет обеспечение безопасности информационной инфраструктуры страны при авариях, катастрофах и стихийных бедствиях. Сокрытие, задержка поступления, искажение и разрушение оперативной информации, несанкционированный доступ к ней отдельных лиц или групп лиц могут привести как к человеческим жертвам, так и к возникновению разного рода сложностей в управлении большими массами людей. Так, могут быть приведены в движение неуправляемые большие массы людей (толпа), испытывающие психологический стресс. На основе слухов, ложной и недостоверное информации могут быстро возникать и распространяться паника и беспорядки.

К специфическим для условий информационного противоборства направлениям обеспечения информационной безопасности в сфере ГО также относятся:

разработка эффективной, защищенной системы мониторинга объектов повышенной опасности;

совершенствование системы информирования населения об угрозах возникновения ЧС, об условиях их возникновения и развития;

повышение надежности систем обработки и передачи информации, обеспечивающих деятельность федеральных органов исполнительной власти в условиях ЧС;

прогнозирование поведения населения в случае появления ложной или недостоверной информации о возможных чрезвычайных ситуациях и разработка профилактических мер;

разработка специальных мер по защите информационных систем, обеспечивающих управление экологически опасными и экономически важными производствами.

В интересах реализации одного из основных направлений обеспечения информационной безопасности и в соответствии с требованиями постановления Правительства Российской Федерации от 1 марта 1993 г. № 178 «О создании локальных систем оповещения в районах размещения потенциально опасных объектов» является создание и поддержание в готовности указанных систем. Оно возложено на ведомства и организации, в ведении которых находятся потенциально опасные объекты.

Специалисты в данной предметной области считают высокой вероятностью появление ложной информации о радиационной, химической, биологической и экологической обстановке в экономически развитых районах России в интересах информационного противоборства. В связи с этим оснащение надежными средствами контроля их состояния является для МЧС России неотложной задачей.

На территории России имеются потенциально опасные объекты, не имеющие и не создающие ло

Информационные угрозы и объекты воздействия	**Основные мероприятия обеспечения информационной безопасности**
Негативное информационное воздействие на мировое общественное мнение с целью дискредитации основ политики России в области защиты населения и территорий в чрезвычайных ситуациях	Систематическое выявление угроз и их источников, структуризация целей обеспечения информационной безопасности в сфере ГО и определение соответствующих практических задач. Снижение эффективности информационного воздействия противника. Противодействие попыткам манипулирования процессами восприятия информации населением со стороны деструктивных сил, противодействие внедряемым целям, мотивам и смыслам деятельности, чуждым национальным интересам государства.
Деструктивное воздействие на общественное сознание населения России негативных факторов, снижающих морально-психологическую устойчивость населения и личного состава формирований ГО их готовность к выполнению задач по защите населения и территорий в чрезвычайных ситуациях	Формирование и поддержание традиционных мировоззренческих основ, целей, ценностей, национальных интересов России в информационном пространстве (глобальном, региональном, национальном). Совершенствование нормативно-правового обеспечения информационной области безопасности в сфере деятельности МЧС России
Психологическое воздействие на население и личный состав формирований гражданской обороны в зоне ЧС	Совершенствование концептуальных походов к основам обеспечения информационной безопасности населения и личного состава формирований ГО. Совершенствование информационно-пропагандистских и психологических приемов и способов работы персонала структурных подразделений МЧС России
Несанкционированный доступ к системе сбора, обработки и передачи оперативной информации в зоне ЧС	Совершенствование средств защиты информации от несанкционированного доступа, развитие защищенных систем связи и управления, повышение надежности специального программного обеспечения. Оптимизация структуры функциональных органов системы обеспечения информационной безопасности в сфере ГО и координация их взаимодействия
Несанкционированный доступ к системам принятия решений по оперативным действиям (реакциям), связанным с развитием ЧС и ходом ликвидации их последствий	Повышение надежности систем обработки и передачи информации, обеспечивающих деятельность федеральных органов исполнительной власти
Хакерские атаки на управленческие программно-аппаратные комплексы	Проведение сертификации общего и специального программного обеспечения, пакетов прикладных программ и средств защиты информации в существующих и создаваемых автоматизированных системах управления связи. Подготовка специалистов в области обеспечения информационной безопасности в сфере ГО и др.
Получение доступа к функционирующим средствам связи для воздействия на управленческие действия и технические средства	Повышение уровня отечественных информационных технологий, внедряемых в средства связи и управления.

кальные системы оповещения. Из них 37,2 % объектов находится в ведении федеральных органов исполнительной власти и организаций Российской Федерации, 46,2 % — в ведении органов исполнительной власти субъектов Российской Федерации и органов местного самоуправления, 38 % — частные предприятия[5].

Оснащение потенциально опасных объектов современными средствами контроля и локальными системами оповещения населения, защищенными от несанкционированного проникновения (особенно РХБ и экологического характера) обусловлено тем, что роль оперативных данных о степени химической, биологической и радиационной опасности в информационном противоборстве переоценить невозможно.

Создание, внедрение и распространение ложной информации — иногда в форме слухов о неблагополучной радиационной, химической и биологической, а в целом и экологической обстановке может быть использовано для возбуждения панических настроений населения и в районах дислокации войск, а также в целях общей дестабилизации обстановки. Одной из ключевых проблем информационной борьбы является защита каналов передачи такого рода сведений.

Практическое выполнение структурными элементами системы МЧС России задач информационного противоборства в ходе ликвидации ЧС на потенциально опасных объектах (особенно РХБ характера) подтверждает необходимость сопровождения таких действий экспертно-аналитическими подразделениями.

Создание таких подразделений позволит повысить оперативность доведения информации о реальной обстановке в зоне ЧС до населения и государственных структур.

Заключение

Стремительные темпы развития компьютеризации и информатизации общества неизбежно ведут к созданию единого мирового информационного пространства. В нем будут аккумулированы все средства сбора, накопления, обработки, хранения и обмена информацией между людьми, организациями и государствами. В XXI веке основу мирового информационного пространства составят национальные информационно-управляющие инфраструктуры развитых государств, таких как США, Китая, стран Западной Европы и Японии. В настоящее время создаются предпосылки значительного роста политического, экономического и военного превосходства развитых индустриальных стран за счет их лидирующей роли в компьютеризации и информатизации.

Вопросы обеспечения национальной и военной безопасности России весьма актуальны, если учесть, что объемы информации, обрабатываемые (добываемые, хранимые, передаваемые и др.) с помощью глобальных информационных сетей, значительно (по разным оценкам в 2,5 — 5 раз) превосходят объемы информации, передаваемой традиционными способами (бумажные носители, видео-, аудиоинформация и др.).

Ресурс информационного и других воздействий потенциально опасных для России государств столь велик, а способы их применения и характер могут быть настолько неожиданными, что только в случае надежной защиты своей информационной среды и возможностей средств противоборства она сможет устоять под мощными информационным, силовым и психологическим ударами противника.

Для МЧС России наиболее уязвимыми объектами в сфере обеспечения информационной безопасности являются системы экстренного оповещения населения о возникновении ЧС, система принятия решений по оперативным действиям (реакциям), связанным с развитием таких ситуаций и ходом ликвидации их последствий, а также система сбора и обработки информации о возможном возникновении ЧС.

Развитие перспективных технологий и разработка современных технических средств, осуществляющих прием, обработку и передачу информации об угрозе возникновения или о возникновении ЧС, защищенных от несанкционированного воздействия, является для МЧС России актуальной задачей.

Литература

- *Шойгу С.К.* и др. Атлас природных и техногенных опасностей рисков ЧС в Российской Федерации. М.: «Дизайн». Информация. Картография, 2005.
- *Багиров А.С.* Интернет в международных отношениях. Международная жизнь, № 8 — 9. 2000. С. 77 — 89.
- *Гриняев С.П.* Концепция ведения информационной войны в некоторых странах мира. Зарубежное военное обозрение, № 2. 2002. С. 98 — 105.
- *Жуков В.* Взгляды военного руководства США на ведение информационной войны. Зарубежное военное обозрение, № 1. 2001.
- *Павлютенкова М.В.* Информационная война — реальная угроза или современный миф? Власть, № 12. 2001. С. 37—59.

21.01.2014

Сведения об авторах:

Фалеев Михаил Иванович: к.п.н.; начальник центра; *Черных Геннадий Сергеевич:* д.в.н.; профессор; Заслуженный работник высшей школы РФ;

ФКу ЦСИ ГЗ МЧС России; e-mail: csi430@yan- dex.ru; 121352, Москва, ул. Давыдковская, д. 7.

Примеры информационных угроз и онлайн мошенничество (по материалам периодической печати)

1. SMS-просьба («я в беде, пришли денег»). Если вы звоните по номеру, откуда пришло сообщение, вам обычно не отвечают.
2. «Ошибочный» перевод. Приходит sms с информацией, что на ваш банковский или телефонный счет перечислена определенная сумма денег. Потом звонит псевдосотрудник банка или сотовой компании, сообщает об ошибке и просит вас вернуть несуществующие деньги.
3. Звонок с запросом кода банковской карты. Человек представляется сотрудником вашего банка. Просит продиктовать номер вашего лицевого счета и ПИН-код карты.
4. SMS-рассылка с предложением «услуг по шпионажу». Есть люди, которые с охотой последили бы за перемещениями близких или прочитали их sms. На деле вместо шпионской услуги неудавшийся Джеймс Бонд получает ноль на счете.
5. «Розыгрыш» призов. От имени популярного теле или радиоведущего вам сообщают о выигрыше крупного приза, для получения которого нужно заплатить налог либо предоплату.
6. Звонок от имени представителя правоохранительных органов. Чаще всего человеку сообщают, что его родственник попал в ДТП. Чтобы окончательно огорошить жертву, преступники могут сообщить, что близкий ему человек, либо получил травму, либо погиб. И потребовать деньги – под предлогом штрафных санкций, например.
7. Российская Армия переходит на компьютерные технологии, в связи с чем возможно в армию поступают ноутбуки-шпионы. Компьютер сам может связываться с базовыми серверами, находящимися за границей, отправлять туда данные с точными координатами конкретного ноутбука.
8. У Нижегородцев скупают личную информацию. Гражданин заключает договор на работу агитатором перед выборами. Выборы проходят, а на его имя можно взять кредит.
9. Онлайновые мошенники, которые обманывают людей, понадеявшихся на легкий заработок в Интернете. И это только одна из угроз, которые поджидают пользователя, когда он начинает активно пользоваться Сетью.
10. По эл.почте приходит письмо с выходом на сайт в соц.сеть Одноклассники или вКонтакте. При помощи поддельных писем и фальшивых сайтов мошенники пытаются разузнать данные о банковских картах.
11. «Негерийские» письма. В ваш эл.почтовый адрес попадает письмо от неизвестного корреспондента. Вам предлагается солидный процент за перевод капиталов «чернокожего миллиардера» с переводов его капиталов за границу. Либо предложение вам стать его наследником и оплатить расходы по пересылки документов или комиссии. Получив деньги мошенники либо скрываются, либо требуют новые вливания.
12. Вы ищите в Internet фильм или аудиокнигу и попадаете на сайт, где якобы нашлось то, что вам нужно. Далее идет «регистрация» и с вашего мобильного списывается пара сотен рублей.
13. Фишинг – это воровство персональных данных жертвы (логин и пароль) якобы от каких-то банков, соц.сетей.
14. Ваш телефон постоянно за вами «следит». И ваши персональные данные могут оказаться в Internet.
15. Перед Олимпиадой фанатам не в коем случае не стоит заказывать билеты по Internet, поскольку высока вероятность нарваться на фишинговый веб-сайт.

«Карточные» фокусы или как воруют деньги с карт:

1. Преступнику нужно не так уж много данных – номер карточки, название банка, три цифры на обороте пластика, имя держателя. Эту информацию мошенники снимают на камеры, но чаще вытягивают у доверчивых граждан по телефону, например, при обсуждении купле-продажи чего-либо. Прочее взломщик раздобудет в Internet сам. Его цель – создание карточки-клона.

2. Нужные данные можно получить и после покупки с рук бывшей в употреблении симки мобильного телефона. Через симку мошенник может получить доступ к счету.

3. Использование устройства ридер – переносной терминал для считывания банковских карт. С помощью ридеров банковские карты считывают прямо в метро или там, где «кучкуются» богатые иностранцы и миллионеры. Это могут делать и недобросовестные продавцы, кассиры, сотрудники банков. После чего также изготавливается карточка-клон.

4. На сотовый телефон приходит sms-сообщение якобы от службы безопасности банка: «вашей картой пытаются воспользоваться», называется место, как правило, большой торговый центр. С банкомата деньги отправляются на счет мошенника.

5. Представленные короткие номера юридическим и физическим лицам, например «900» может оказаться номером 90+буква О.

О РУССКОМ ХАКЕРЕ, БЕССМЫСЛЕННОМ И БЕСПОЩАДНОМ

Окончание. Начало на с. 1

ДЕСЯТКИ лет домо-рощенные строители информационных сетей пользуются американским оборудованием. Сам чёрт не знает, что в нём внутри и что произойдёт, если кем-то извне будет дана команда хотя бы по остановке его работы или работе в режиме «глюков и запаздывания», что ещё хуже. В один миг «американские настоящие хакеры» могут остановить наши электростанции, заблокировать подачу тепла и электричества в лютую стужу, остановить работу аэропортов и железной дороги и чёрт-те что ещё! Это вам не взлом сервера Демпартии США, это чистый кирдык, который может случиться в любой момент.

Самое время почесать репу и задуматься – почему они до сих пор этого не сделали? Ответ очевиден – боятся атомной бомбы. Она тоже работает, как хакер. При взрыве на высоте в километр где-нибудь над Нью-Йорком можно одновременно распылить графитную пыль. Всё, что работает на электричестве, почти сразу сломается – от коротких замыканий. Но это будет означать начало «горячей войны», что крайне нежелательно. С другой стороны, американский государственный хакер и его хозяин должны знать, что возмездие может наступить из космоса и без применения атомного оружия. На современном языке это называется Использование Радиоэлектронных Средств (РЭБ). С ними у нас всё не так плохо – научились так искажать электронные по-

можем сделать слепыми и неуправляемыми.

Осталось решить главную задачу – дать понять командирам американских хакеров, что их возможные проделки до добра не доведут. Что неотвратимы удар возмездия и удачное завершение Судного дня. Это когда российские межконтинентальные ядерные ракеты уверенно смогут долететь до вражеской территории и их не уничтожат на активном участке полёта с помощью американской ПРО из Аляски и Польши. Только это и может пока остановить настоящих американских хакеров.

И здесь самое время напомнить ещё раз, что вот этого у нас как раз и не хватает. Программа по развёртыванию тяжёлых спутниковых систем закрыта два года назад, а по созданию сверхтяжёлых носителей даже не начата. Именно они могли бы парализовать любую зону над земной поверхностью и сделать американскую ПРО бесполезной. Но идеолог создания этой оборонной системы член-корреспондент РАН и доктор технических наук **Виталий Лопота** так и находится под следствием по чёрному навету, хотя с него и сняли позорный тюремный браслет. Тем временем «Роскосмос» продолжает модернизировать космическую технику 50-х годов прошлого века.

Другой задачи нашим учёным пока не поставлено. «Самому» явно не до фантастических сюжетов будущего – против него сегодня весь «западный» мир. А новая российская знать, в том числе и политическая, в такую ерунду, как «хакерские» атаки, скорее всего, просто не верит.

2. Вредоносные программы

«Бойтесь данайцев, дары приносящих»

Под вредоносными программами в дальнейшем будем понимать такие программы, которые прямо или косвенно дезорганизуют процесс обработки информации или способствуют утечке или искажению информации.

Ниже рассмотрим некоторые (самые распространенные) виды подобных программ:

«Троянский конь» - программа, выполняющая в дополнение к основным (проектным и документированным) не описанные в документации действия. Аналогия с

древнегреческим «троянским конем» таким образом, вполне оправдана - в не вызывающей подозрений оболочке таится угроза.

Опасность «троянского коня» заключается в дополнительном блоке команд, тем или иным образом вставленном в исходную безвредную программу, которая затем предлагается (дарится, продается, подменяется) пользователем. Этот блок команд может срабатывать при наступлении некоторого условия (даты, времени и т.д., либо по команде извне).

Наиболее опасные действия «троянский конь» может выполнять, если запустивший ее пользователь обладает расширенным набором привилегий. В этом случае злоумышленник, составивший и внедривший «троянского коня», и сам этими привилегиями не обладающий, может выполнить несанкционированные привилегированные функции чужими руками. Или, например, злоумышленника очень интересуют наборы данных пользователя, запустившего такую программу. Последний может даже не обладать расширенным набором привилегий - это не помешает выполнению несанкционированных действий.

Вирус - это программа, которая может заражать другие программы путем включения в них своей, возможно модифицированной, копии, причем последняя сохраняет способность к дальнейшему размножению.

Своим названием компьютерные вирусы обязаны определенному сходству с вирусами биологическими:

- способностями к саморазмножению;
- высокой скорости распространения;
- избирательности поражаемых систем (каждый вирус поражает только определенные системы или однородные группы систем);
- наличию в большинстве случаев определенного инкубационного периода;
- способности «заражать» еще незараженные системы;
- трудности борьбы с вирусами и т.д.

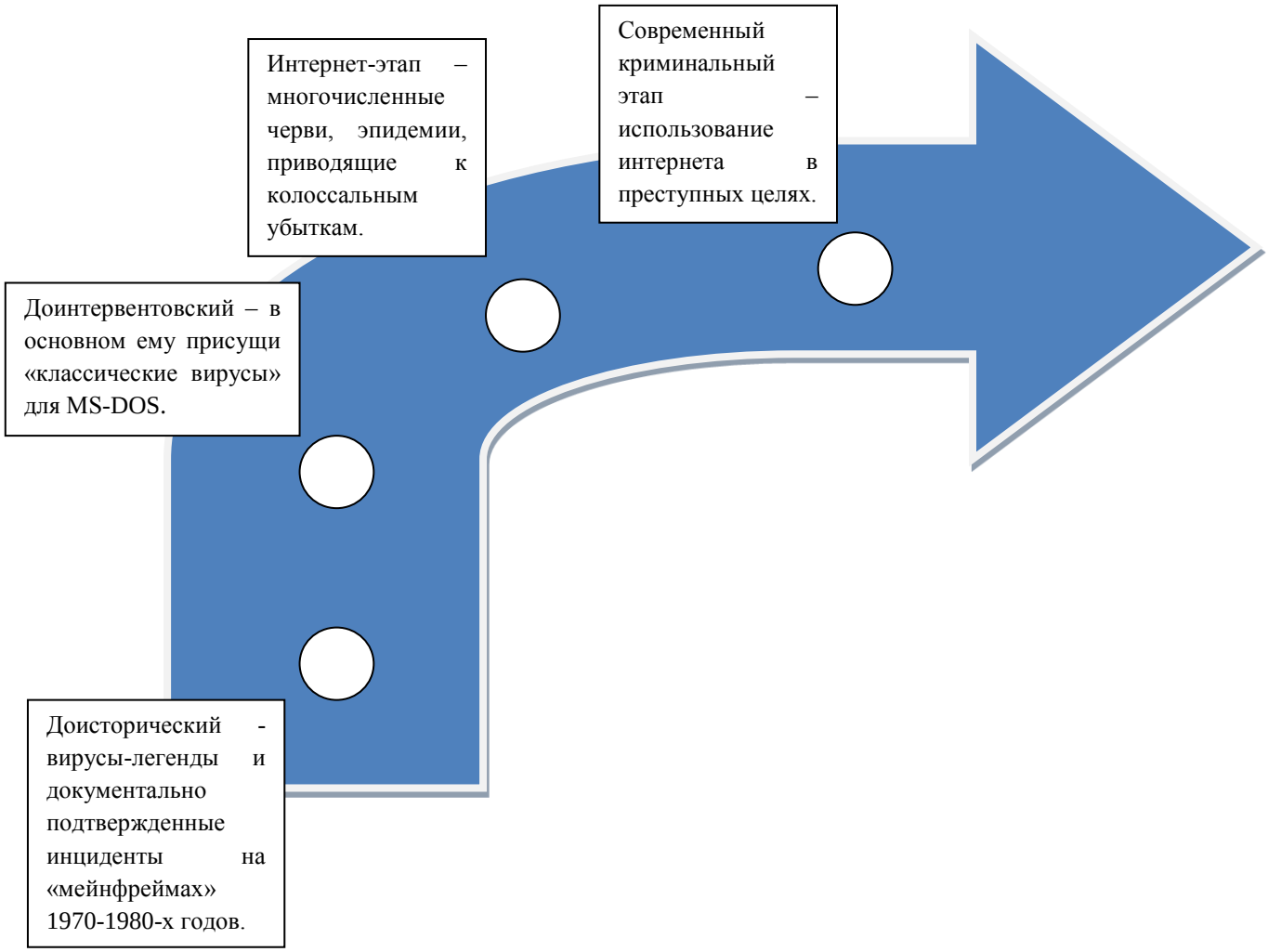


Рис. 8. История компьютерных вирусов.

Среда обитания	Сетевые	Распространяются по компютерной сети
	Файловые	Внедряются в выполняемые файлы
	Загрузочные	Внедряются в загрузочный сектор диска (Boot-сектор)

Рис. 9. Основные классы вирусов.

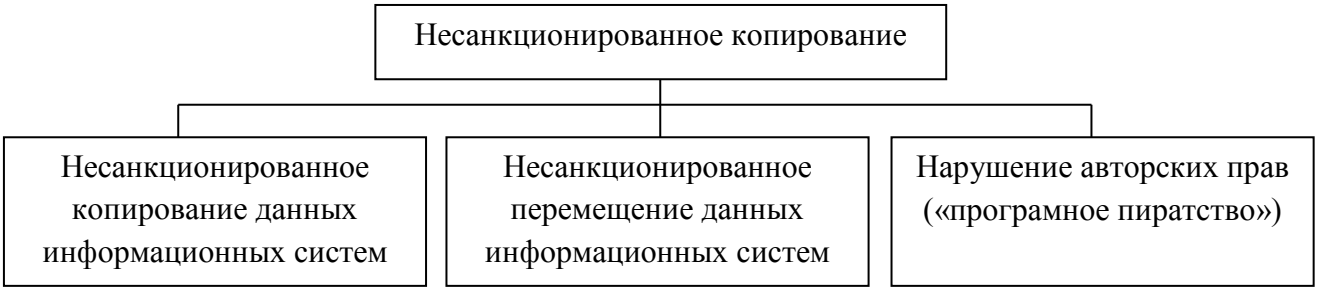


Рис. 10. Копирование информации.

В последнее время к этим особенностям, характерным для вирусов компьютерных и биологических, можно добавить еще и постоянно увеличивающуюся быстроту появления модификаций и новых поколений вирусов, что можно объяснить идеями злоумышленников определенного склада ума.

Программа, внутри которой находится вирус, называется «зараженной». Когда такая программа начинает работу, то сначала управление получает вирус. Вирус находит и «заражает» другие программы, а также выполняет какие-нибудь вредные действия.

Процесс заражения вирусом программных файлов можно представить следующим образом. В зараженной программе код последней изменяется таким образом, чтобы вирус получил управление первым, до начала работы программы- вирусоносителя. При передаче управления вирусу он каким-либо способом находит новую программу и выполняет вставку собственной копии в начало или добавление ее в конец этой, обычно еще не зараженной, программы. Если вирус записывается в конец программы, то он корректирует код программы с тем, чтобы получить управление первым. После этого управление передается программе-вирусоносителю, и та нормально выполняет свои функции. Более изощренные вирусы могут для получения управления изменять системные области накопителя (например, сектор каталога), оставляя длину и содержимое заражаемого файла без изменений.

Загрузочные вирусы. От файловых вирусов загрузочные вирусы отличаются методом распространения. Они поражают не программные файлы, а определенные системные области магнитных носителей (гибких и жестких дисков). На включенном компьютере они могут временно располагаться в оперативной памяти.

Обычно поражение происходит при попытке загрузки компьютера с магнитного носителя, системная область которого содержит загрузочный вирус. Так, например, при попытке загрузить компьютер с гибкого диска происходит сначала проникновение вируса в оперативную память, а затем в загрузочный сектор жестких дисков. Далее этот компьютер сам становится источником распространения загрузочного вируса.

Макровирусы. Эта особая разновидность вирусов поражает документы, выполненные в некоторых прикладных программах, имеющих средства для исполнения так называемых макрокоманд.

В частности, к таким документам относятся документы текстового процессора MicrosoftWord. Заражение происходит при открытии файла документа в окне программы, если в ней не отключена возможность исполнения макрокоманд.

«Червь» - программа, распространяющаяся через сеть и не оставляющая своей копии на магнитном носителе. «Червь» использует механизмы поддержки сети для определения узла, который может быть заражен. Затем с помощью тех же механизмов передает свое тело или его часть на этот узел и либо активизируется, либо ждет для этого подходящих условий.

Наиболее известный представитель этого класса - вирус Морриса (или, вернее, «червь Морриса»), поразивший сеть Internetв 1988 г. Наиболее подходящей средой распространения «червя» является сеть, все пользователи которой считаются дружественными и доверяют друг другу. Отсутствие защитных механизмов как нельзя лучше способствует уязвимости сети.

«Жадные» программы - это программы, которые при выполнении стремятся монополизировать какой-либо ресурс системы, не давая другим программам возможности использовать его. Доступ таких программ к ресурсам системы обычно приводит к нарушению ее доступности. Естественно, такая атака будет активным вмешательством в работу системы. Непосредственной атаке обычно подвергаются ключевые объекты системы: процессор, оперативная память, устройства ввода-вывода.

Тупиковая ситуация возникает, когда «жадная» программа бесконечна (например, исполняет заведомо бесконечный цикл). Однако во многих операционных системах существует возможность ограничения времени процессора, используемого задачей. Это не относится к операциям, выполняющимся в зависимости от других программ, например, к операциям ввода-вывода, которые завершаются асинхронно к основной программе; время их выполнения не включается в счет времени программы. Перехватывая сообщение о завершении операции ввода-вывода и посылая вновь запрос на новый ввод-вывод, можно добиться по-настоящему бесконечной программы.

Другой пример «жадной» программы - программа, захватывающая слишком большую область оперативной памяти. В оперативной памяти последовательно размещаются данные, например подкачиваемые с внешнего носителя. В конце концов память может оказаться во владении одной программы, и выполнение других окажется невозможным.

Что такое шпионские программы?

Как следует из названия, эти программы предназначены для сбора данных и отправки их третьей стороне без вашего ведома и согласия. Такие программы могут отслеживать нажатия клавиш (клавиатурные шпионы), собирать конфиденциальную информацию (пароли, номера кредитных карт, PIN-коды и т.д.), отслеживать адреса электронной почты в почтовом ящике или особенности вашей работы в Интернете. Кроме того, шпионские программы неизбежно снижают производительность компьютера.

Захватчики паролей. Это программы специально предназначены для воровства паролей. При попытке входа имитируется ввод имени и пароля, которые пересылаются владельцу программы-захватчика, после чего выводится сообщение об ошибке ввода и управление возвращается операционной системе. Пользователь, думающий, что допустил ошибку при наборе пароля, повторяет вход и получает доступ к системе. Однако его имя и пароль уже известны владельцу программы-захватчика. Перехват пароля может осуществляться и другим способом - с помощью воздействия на программу, управляющую входом пользователей в систему и ее наборы данных.

Методика воздействия вредоносных программ в значительной мере зависит от организации обработки информации в системе, разработанной политики безопасности, возможностей установленных средств защиты, а также добросовестности администратора и оператора. Для реализации НСД существует два способа:

-во-первых, можно преодолеть систему защиты, то есть путем различных воздействий на нее прекратить ее действия в отношении себя или своих программ. Это сложно, трудоемко и не всегда возможно, зато эффективно;

- во-вторых, можно понаблюдать за тем, что «плохо лежит», то есть какие наборы данных, представляющие интерес для злоумышленника, открыты для доступа по недосмотру или умыслу администратора. Такой доступ, хотя и с некоторой натяжкой, тоже можно назвать несанкционированным, его легко осуществить, но от него легко и защититься. К этому же типу относится НСД с подбором пароля, поскольку осуществить такой подбор возможно лишь в случае нарушения правил составления паролей и использования в качестве пароля человеческих имен, повторяющихся символов и пр.

В подавляющем большинстве случаев НСД становится возможным из-за непродуманного выбора средств защиты, их некорректной установки и настройки, плохого контроля работы, а также при небрежном отношении к защите своих собственных данных.

Незаконное использование привилегий

Злоумышленники, применяющие данный способ атаки, обычно используют штатное программное обеспечение (системное или прикладное), функционирующее в нештатном режиме. Практически любая защищенная система содержит средства, используемые в чрезвычайных ситуациях, при сбоях оборудования или средства, которые способны функционировать с нарушением существующей политики безопасности. В некоторых случаях пользователь должен иметь возможность доступа ко всем наборам системы (например, при внезапной проверке).

Такие средства необходимы, но они могут быть чрезвычайно опасными. Обычно эти средства используются администраторами, операторами, системными программистами и другими пользователями, выполняющими специальные функции.

Для того чтобы уменьшить риск от применения таких средств большинство систем защиты реализует такие функции с помощью набора привилегий - для выполнения определенной функции требуется определенная привилегия. В этом случае каждый пользователь получает свой набор привилегий, обычные пользователи - минимальный, администраторы - максимальный (в соответствии с принципом минимума привилегий).

Естественно, при таких условиях расширенный набор привилегий - заветная мечта любого злоумышленника. Он позволит ему совершать практически любые действия, причем, возможно, даже в обход всех мер контроля. Нарушения, совершаемые с помощью незаконного использования привилегий, являются активным воздействием, совершаемым с целью доступа к какому-либо объекту или системе в целом.

Незаконный захват привилегий возможен либо при наличии ошибок в самой системе защиты (что, например, оказалось возможным в одной из версий операционной системы UNIX), либо в случае халатности при управлении системой и привилегиями в частности (например, при назначении расширенного набора привилегий всем подряд).

Атаки «салями»

Атаки «салями» более всего характерны для систем, обрабатывающих денежные счета и, следовательно, для банков особенно актуальны. Принцип атак «салями» построен на том факте, что при обработке счетов используются целые единицы (центы, рубли, копейки), а при исчислении процентов нередко получаются дробные суммы.

Например, 6,5% годовых от $102,87 за 31 день составит $0,5495726. Банковская система может округлить эту сумму до $0.55. Однако если пользователь имеет доступ к банковским счетам или программам их обработки, он может округлить ее в другую сторону - до $0.54, а разницу в 1 цент записать на свой счет. Владелец счета вряд ли ее заметит, а если и обратит внимание, то спишет ее на погрешности обработки и не придаст значения. Злоумышленник же получит прибыль в один цент, при обработке 10.000 счетов в день. Его прибыль таким образом составит $1000, т.е. около $300 000 в год.

Отсюда и происходит название таких атак - как колбаса салями изготавливается из небольших частей разных сортов мяса, так и счет злоумышленника пополняется за счет различных вкладчиков. Естественно, такие атаки имеют смысл лишь в тех организациях, где осуществляется не менее 5000 - 10000 транзакций в день, иначе не имеет смысла рисковать, поскольку в случае обнаружения преступника просто определить. Таким образом, атаки «салями» опасны в основном для крупных банков.

Причинами атак «салями» являются, во-первых, погрешности вычислений, позволяющие трактовать правила округления в ту или иную сторону, а во-вторых, огромные объемы вычислений, необходимые для обработки счетов. Успех таких атак зависит не столько от величины обрабатываемых сумм, сколько от количества счетов (для любого счета погрешность обработки одинакова). Атаки «салями» достаточно трудно распознаются, если только злоумышленник не начинает накапливать на одном счете миллионы.

«Скрытые каналы»

«Скрытые каналы» - пути передачи информации между процессами системы, нарушающие системную политику безопасности. В среде с разделением доступа к информации пользователь может не получить разрешение на обработку интересующих его данных, однако может придумать для этого обходные пути. Практически любое действие в системе каким-то образом затрагивает другие ее элементы, которые при этом могут изменять свое состояние. При достаточной наблюдательности и знании этих связей можно получить прямой или опосредованный доступ к данным.

«Скрытые каналы» могут быть реализованы различными путями, в частности при помощи программных закладок («троянских коней»).

Например, программист банка не всегда имеет доступ к именам и балансам депозитных счетов. Программист системы, предназначенной для обработки ценных бумаг, может не иметь доступ к предложениям о покупке или продаже. Однако при создании таких систем он может предусмотреть способ получения интересующих его сведений. В этом случае программа скрытым способом устанавливает канал связи с этим программистом и сообщает ему требуемые сведения.

Атаки с использованием скрытых каналов обычно приводят к нарушениям конфиденциальности информации, по характеру воздействия являются пассивными, нарушение состоит только в передаче информации. Для организации «скрытых каналов» может использоваться как штатное программное обеспечение, так и специально разработанные «троянские» или вирусные программы. Атака обычно производится программным способом.

«Скрытым каналом» может явиться передача информации о наличии или отсутствии какого-либо набора данных, его размере, дате создания или модификации и т.д.

Также существует большое количество способов организации связи между двумя процессами системы. Более того, многие операционные системы имеют в своем распоряжении такие средства, так как они очень облегчают работу программистов и пользователей. Проблема заключается в том, что очень трудно отделить неразрешенные «скрытые каналы» от разрешенных, то есть тех, которые не запрещаются системной политикой безопасности. В конечном счете все определяется ущербом, который может принести организация «скрытых каналов».

Отличительными особенностями «скрытых каналов» является их малая пропускная способность (по ним обычно можно передавать только небольшое количество информации), большие трудности их организации и обычно небольшой наносимый ими ущерб.

«Маскарад»

Под «маскарадом» понимается выполнение каких-либо действий одним пользователем от имени другого пользователя. При этом такие действия другому

пользователю могут быть разрешены. Нарушение заключается в присвоении прав и привилегий.

Цель «маскарада» - сокрытие каких-либо действий за именем другого пользователя или присвоение прав и привилегий другого пользователя для доступа к его наборам данных или для использования его привилегий.

«Маскарад» - это способ активного нарушения защиты системы, он является опосредованным воздействием, то есть воздействием, совершенным с использованием возможностей других пользователей.

Примером «маскарада» может служить вход в систему под именем и паролем другого пользователя, при этом система защиты не сможет распознать нарушение. В этом случае «маскараду» обычно предшествует взлом системы или перехват пароля.

Другой пример «маскарада» - присвоение имени другого пользователя в процессе работы. Это может быть сделано с помощью средств операционной системы (некоторые операционные системы позволяют изменять идентификатор пользователя в процессе работы) или с помощью программы, которая в определенном месте может изменить определенные данные, в результате чего пользователь получит другое имя. В этом случае «маскараду» может предшествовать захват привилегий, или он может быть осуществлен с использованием какой-либо ошибки в системе.

«Маскарадом» также называют передачу сообщений в сети от имени другого пользователя. Способы замены идентификатора могут быть разные, обычно они определяются ошибками и особенностями сетевых протоколов. Тем не менее на приемном узле такое сообщение будет воспринято как корректное, что может привести к серьезным нарушениям работы сети. Особенно это касается управляющих сообщений, изменяющих конфигурацию сети, или сообщений, ведущих к выполнению привилегированных операций.

Наиболее опасен «маскарад» в банковских системах электронных платежей, где неправильная идентификация клиента может привести к огромным убыткам. Особенно это касается платежей с помощью электронных банковских карт. Сам по себе метод идентификации с помощью персонального идентификатора (PIN) достаточно надежен, нарушения могут происходить вследствие ошибок его использования. Это произойдет, например, в случае утери кредитной карты, при использовании очевидного идентификатора (своего имени, ключевого слова и т.д.). Поэтому клиентам надо строго соблюдать все рекомендации банка по выполнению такого рода платежей.

«Сборка мусора»

После окончания работы обрабатываемая информация не всегда полностью удаляется из памяти. Часть данных может оставаться в оперативной памяти, на дисках и лентах, других носителях. Данные хранятся на носителе до перезаписи или уничтожения; при выполнении этих действий на освободившемся пространстве диска находятся их остатки. Хотя прочитать такие данные трудно, однако, используя специальные программы и оборудование, все же возможно. Такой процесс принято называть «сборкой мусора». Он может привести к утечке важной информации.

«Взлом системы»

Под «взломом системы» понимают умышленное проникновение в систему с несанкционированными параметрами входа, то есть именем пользователя и его паролем (паролями).

«Взлом системы» - умышленное, активное воздействие на систему в целом. «Взлом системы» обычно происходит в интерактивном режиме.

Поскольку имя пользователя не является секретом, объектом «охоты» обычно становится пароль. Способы вскрытия пароля могут быть различны: перебор

возможных паролей, «маскарад» с использованием пароля другого пользователя, захват привилегий. Кроме того, «взлом системы» можно осуществить, используя ошибки программы входа.

«Люки»

Люком называется не описанная в документации на программный продукт возможность работы с этим программным продуктом. Сущность использования люков состоит в том, что при выполнении пользователем некоторых не описанных в документации действий он получает доступ к возможностям и данным, которые в обычных условиях для него закрыты (в частности - выход в привилегированный режим).

«Люки» чаще всего являются результатом забывчивости разработчиков. В частности, отладка программы ведется за счет прямого доступа к отдельным частям продукта или наборе определенного сочетания клавиш.

Одним из наиболее показательных примеров использования «забытых» люков является, пожалуй, широко известный в компьютерном мире вирус Морриса. Одной из причин, обусловивших возможность распространения этого вируса, была ошибка разработчика программы электронной почты. По оценкам американских специалистов, ущерб нанесенный в результате этого инцидента, составил более чем 100 миллионов долларов.

Вообще люк (или люки) могут присутствовать в программе в виду того, что программист:

- забыл удалить его;
- умышленно оставил его в программе для обеспечения тестирования или выполнения оставшейся части отладки;
- умышленно оставил его в программе в интересах облегчения окончательной сборки конечного программного продукта;
- умышленно оставил его в программе с тем, чтобы иметь скрытое средство доступа к программе уже после того, как она вошла в состав конечного продукта.

В первом случае «люк» - неумышленная, но серьезная брешь в безопасности системы. Во втором и третьем случаях «люк» - серьезная экспозиция безопасности системы. Наконец, в последнем случае «люк» - первый шаг к атаке системы.

В любом случае «люк» - это возможность получить управление системой в обход защиты.

Отметим, что программная ошибка «люком» не является. «Люк» - это достаточно широко используемый механизм отладки, корректировки и поддержки программ, который создается преднамеренно, хотя чаще всего и без злого умысла. Люк становится опасным, если он не замечен, оставлен и не предпринималось никаких мер по контролю за ним.

«Логической бомбой» называют участок программы, который реализует некоторые действия при наступлении определенных условий в дате или имени файла.

Мировая компьютерная общественность достаточно хорошо знакома с «логическими бомбами». Логическая бомба является одним из излюбленных способов мести программистов Компаниям, которые их уволили или чем-либо обидели. При этом чаще всего срабатывание бомбы становится в зависимость от установки в системе даты - так называемые «часовые» бомбы. Это очень удобно: допустим, программист знает, что его уволят 1 февраля. В таком случае он может установить «часовую» бомбу на взрыв, допустим 6 мая, когда сам он будет уже вне пределов досягаемости для пострадавшей компании.

После ее запуска на экране дисплея можно увидеть мультипликационные картинки с американской певицей Мадонной, причем показ завершается выдачей сообщения следующего содержания «Только идиот использует свой компьютер для того, чтобы рассматривать видеозвезд!». Во время демонстрации бомба удаляет себя, но заодно удаляет и все файлы на доступных для нее дисках.

Эксперты считают, что на сегодняшний день число существующих вирусов перевалило за 50 тысяч, причем ежедневно появляется от 6 до 9 новых. Реально циркулирующих вирусов в настоящее время насчитывается около более 200.

Один из авторитетнейших «вирусологов» страны Евгений Касперский предлагает условно классифицировать вирусы по следующим признакам:

- по среде обитания вируса;
- по способу заражения среды обитания;
- по деструктивным возможностям;
- по особенностям алгоритма вируса.

Более подробная классификация внутри этих групп представлена на рис. 4.

Среда обитания	Сетевые	Распространяются по компьютерной сети
	Файловые	Внедряются в выполняемые файлы
	Загрузочные	Внедряются в загрузочный сектор диска (Boot-сектор)

Рис. 11. Основные классы вирусов.

Способы заражения	
Резидентные	Находятся в памяти, активны до выключения компьютера
Нерезидентные	Не заражают память, являются активными ограниченное время
Безвредные	Практически не влияют на работу; уменьшают свободную память на диске в результате своего размножения
Неопасные	Уменьшают свободную память, создают звуковые, графические и прочие эффекты
Опасные	Могут привести к потере программ или системных данных
Очень опасные	Уменьшают свободную память, создают звуковые, графические и прочие эффекты
Особенности алгоритма вируса	
Вирусы-«спутники»	Вирусы, не изменяющие файлы, создают для EXE-файлов файлы-спутники с расширением .com
Вирусы-«черви»	Распространяются по сети, рассылают свои копии, вычисляя сетевые адреса
«паразитические»	Изменяют содержимое дисковых секторов или файлов
«стелс»-вирусы («невидимки»)	Перехватывают обращения операционной системы к пораженным файлам или секторам и подставляют вместо себя незараженные участки
Вирусы-призраки	Не имеют ни одного постоянного участка кода, труднообнаруживаемы, основное тело вируса зашифровано
Макровирусы	Пишутся не в машинных кодах, а на WordBasik, живут в документах Word, переписывают себя в Normal.dot

Основными путями проникновения вирусов в компьютер являются съемные диски (гибкие и лазерные), а также компьютерные сети. При заражении компьютера вирусом важно его обнаружить по характерным признакам.

Признаками воздействия вирусов на компьютерную систему служат следующие:

- изменение даты создания и длины файла;
- пропажа файла;
- слишком частые обращения к диску;
- непонятные ошибки;
- «зависание» компьютера;
- самопроизвольная перезагрузка операционной системы;
- замедление работы процессора;
- появление неожиданных графических и звуковых эффектов;

- сообщения антивирусных программ.

Все действия вируса могут выполняться достаточно быстро и без выдачи каких-либо сообщений, поэтому пользователю очень трудно заметить, что в компьютере происходит что-то необычное.

Пока на компьютере заражено относительно мало программ, наличие вируса может быть практически незаметно. Однако по прошествии некоторого времени на компьютере начинает твориться что-то странное, например:

- некоторые программы перестают работать или начинают работать неправильно;
- на экран выводятся посторонние сообщения, символы и т.д.;
- работа на компьютере существенно замедляется;
- некоторые файлы оказываются испорченными и т.д.

К этому моменту, как правило, уже достаточно много (или даже большинство) программ являются зараженными вирусом, а некоторые файлы и диски - испорченными. Более того, зараженные программы с одного компьютера могли быть перенесены с помощью дискет или по сети на другие компьютеры.

Некоторые виды вирусов ведут себя еще более коварно. Они вначале незаметно заражают большое число программ или дисков, а потом причиняют очень серьезные повреждения, например, формируют весь жесткий диск на компьютере. А бывают вирусы, которые стараются вести себя как можно более незаметно, но понемногу и постепенно портят данные на жестком диске компьютера.

Большинство вирусов не выполняет каких-либо действий, кроме своего распространения (заражения других программ, дисков и т.д.) и. иногда, выдачи каких-либо сообщений или иных эффектов, придуманных автором вируса: игры, музыки, перезагрузки компьютера, выдачи на экран разных рисунков, блокировки или изменения функций клавиш клавиатуры, замедления работы компьютера и т.д. Однако сознательной порчи информации эти вирусы не осуществляют. Такие вирусы условно называются ***неопасными***. Впрочем, и эти вирусы способны причинить большие неприятности (например, перезагрузки каждые несколько минут вообще не дадут вам работать).

Однако около трети всех видов вирусов портят данные на дисках - или сознательно, или из-за содержащихся в вирусах ошибок, скажем, из-за не вполне корректного выполнения некоторых действий. Если порча данных происходит лишь эпизодически и не приводит к тяжелым последствиям, то вирусы называются ***опасными***. Если же порча данных происходит часто или вирусы причиняют значительные разрушения (форматирование жесткого диска, систематическое изменение данных на диске и т.д.), то вирусы называются ***очень опасными***.

История компьютерной вирусологии представляется сегодня постоянной «гонкой за лидером», причем, не смотря на всю мощь современных антивирусных программ, лидерами являются именно вирусы. Среди тысяч вирусов лишь несколько десятков являются оригинальными разработками, использующими действительно принципиально новые идеи. Все остальные - «вариации на тему». Но каждая оригинальная разработка заставляет создателей антивирусов приспосабливаться к новым условиям, догонять вирусную технологию.

Первые исследования саморазмножающихся искусственных конструкций проводились в середине прошлого столетия. Термин «компьютерный вирус» появился позднее - официально его автором считается сотрудник Лехайского университета США Ф.Коэн, который ввел его в 1984 году на 7-й конференции по безопасности информации.

В 1989 г. американский студент сумел создать вирус, который вывел из строя около 6 000 компьютеров Министерства обороны США. Или эпидемия известного вируса Dir-II, разразившаяся в 1991 году. Вирус использовал действительно оригинальную, принципиально новую технологию и на первых порах сумел широко распространиться за счет несовершенства традиционных антивирусных средств.

Кристоферу Пайну удалось создать вирусы Pathogen и Queen, а также вирус Smeg. Именно последний был самым опасным, его можно было накладывать на первые два вируса и из-за этого после каждого прогона программы они меняли конфигурацию. Поэтому их было невозможно уничтожить. Чтобы распространить вирусы, Пайн скопировал компьютерные игры и программы, заразил их, а затем отправил обратно в сеть. Пользователи загружали в свои компьютеры, зараженные программы и инфицировали диски. Ситуация усугубилась тем, что Пайн умудрился занести вирусы и в программу, которая с ними боролась. Запустив ее, пользователи вместо уничтожения вирусов получали еще один. В результате действий этого вируса были уничтожены файлы множества фирм, убытки составили миллионы фунтов стерлингов.

Широкую известность получил американский программист Моррис. Он известен как создатель вируса, который в ноябре 1988 года заразит порядка 7 тысяч персональных компьютеров, подключенных к Internet.

Убытки от разрушительных последствий вирусных эпидемий, с завидной постоянностью вспыхивающих на просторах Всемирной сети, несут многие крупные интернет-компании, для которых даже несколько часов простоя оборачиваются многомиллионными потерями.

Ведь в результате воздействия некоторых, самых агрессивных из них, может быть не только полностью или частично потеряна информация на жестких или сетевых дисках, но даже могут выйти из строя отдельные микросхемы! Впрочем, существуют и такие, на первый взгляд, вполне безобидные вирусы, которые ничем другим не занимаются, кроме как своим размножением. Однако спустя какое-то время, когда все свободное дисковое пространство будет ими «засорено», производительность системы резко уменьшится.

В последнее время многие из вирусописателей «перепрофилировались». Если раньше подавляющее большинство вирусов создавались исключительно с хулиганскими целями, то сегодня производство вирусов уже превратилось в целую индустрию, приносящую, кстати, ее хозяевам немалый доход. Поэтому «отсталые» вирусы, только и умеющие, что наносить вред операционной системе или приложениям, нынче активно замещают «троянские кони» - программы, предназначенные для хищения конфиденциальной информации, в первую очередь финансового характера.

При этом пользователь зачастую даже и не подозревает, что стал жертвой. В одно мгновение все пароли и данные кредитных карточек, введенные при совершении покупок через Интернет, могут стать добычей третьих лиц.

Вирусописатели демонстрируют готовность не только к изобретению новых технологий, но и к дальнейшему освоению старых.

Мобильные вирусы

Как и предсказывалось, все большие обороты набирает развитие червей и троянцев для мобильных телефонов. В настоящий момент количество вредоносных программ увеличивается примерно на 1 новую программу в неделю.

Примечателен тот факт, что в антивирусные базы были добавлены представители нового класса червей для мобильных телефонов под управлением операционной системы Symbian. Речь идет о «почтовых мобильных червях», использующих для самораспространения MMS (сервис передачи мультимедийных сообщений). В обнаруженные экземпляры встроено два способа распространения. Первый, уже ставший традиционным для мобильных червей, через протокол Bluetooth; червь распространяется, рассылая себя на все доступные устройства в радиусе 10-15 метров. Второй - при помощи MMS - сообщений.

В настоящий момент известно два семейства MMS-червей:

- Comwar, который рассылает себя по всей адресной книге мобильного телефона;
- Cabir.k, который ведет себя более оригинально, а именно - ждет прихода на телефон SMS- или MMS-сообщения и отправляет себя в ответ на него.

Начавшись с одного единственного Bluetooth-червя, вредоносные программы для мобильных устройств сейчас представлены сразу 3-мя классами: Worm (причем, здесь теперь есть как «сетевые» черви, так и «почтовые»), Virus, Trojan.

Если традиционным вирусам потребовались годы, чтобы прийти к такому количеству поведений, то мобильные вирусы проделали этот путь менее чем за год.

Можно с уверенностью прогнозировать, что в ближайший год появятся мобильные представители других классов компьютерных вирусов.

Справочник угроз при работе в интернет

В прошлом компьютерам угрожали преимущественно вирусы и черви. Основной целью этих программ было самораспространение; некоторые программы также причиняли вред файлам и самим компьютерам. Такие вредоносные программы - типичные проявления кибервандализма.

В чем разница между вирусом и червем?

Вирус - это саморазмножающаяся программа, она распространяется с файла на файл и с компьютера на компьютер. Кроме того, вирус может быть запрограммирован на уничтожение или повреждение данных.

Черви считаются подклассом вирусов, но обладают характерными особенностями. Червь размножается (воспроизводит себя), не заражая другие файлы. Он внедряется один раз на конкретный компьютер и ищет способы распространиться далее на другие компьютеры.

Вирус заражает тем большее количество файлов, чем дольше он находится на компьютере необнаруженным. Червь создает единственную копию своего кода. В отличие от вируса, код червя самостоятелен. Другими словами, червь - это отдельный файл, в то время как вирус - это код, который внедряется в существующие файлы.

Что такое рекламные системы (adware)?

Понятие «adware» включает в себя программы, запускающие рекламу (часто в виде всплывающих окон) или перенаправляющие поисковые запросы на рекламные веб-сайты. Рекламное ПО часто бывает встроено в бесплатные или условно-бесплатные программы и устанавливается на компьютер пользователя одновременно с основным приложением без ведома и согласия пользователя. В некоторых случаях рекламное ПО может тайно загрузить и установить на ваш компьютер троянская программа.

Устаревшие, не обновленные вовремя версии веб-браузеров могут быть уязвимыми для хакерских инструментов, скачивающих рекламные программы на ваш компьютер.

Заплатить за свое

Включив компьютер, наш читатель Александр Б. вместо привычной заставки увидел надпись, требующую для нормальной загрузки послать **СМС-сообщение стоимостью 300 руб.**

Он позвонил знакомым программистам с просьбой о помощи. Приехавший компьютерщик переустановил на компьютере программу. Но теперь в машине **вся имеющаяся информация превратилась в страшную абракадабру**. А вирус, который был причиной катастрофы, опять требовал СМС за 300 руб. Время и силы, требуемые для расшифровки необходимых для работы данных, не шли ни в какое сравнение с ценой, названной виртуальными вымогателями. Однако вместо одного сообщения Александру пришлось отправить почти десяток СМС. **Общая сумма снятых с мобильного счета средств составила 2 620 руб.** И только после этого компьютер «заговорил» нормальным языком. При этом тот самый программист выразил сомнение, что проблема не повторится вновь через какое-то время. И рассказал, что ходят слухи о том, что вскоре подобные ситуации начнут происходить не только с компьютерами. Но и со смартфонами и коммуникаторами. Причем в этом случае вирус будет автоматически рассылать сам себя по записной книжке трубки, что приведет к глобальной эпидемии в мире сотовой связи. Чтобы этого не случилось, всем пользователям мобильных телефонов стоит заранее установить на свои трубки **специальные антивирусные программы.**

Дополнительный материал для самостоятельной работы.

Современные вирусы-вымогатели

Начать статью про современные компьютерные вирусы хочется с разговора с одним из их авторов. Не то чтобы очень известный хакер, но человек в «железе» и программах разбирался, а пару его детищ были в базе Касперского. Так вот, на вопрос «зачем он пишет эти программы» получил вполне исчерпывающий ответ – «для интереса». Но было это 10 лет назад. Тогда создавались вирусы-приколы просто блокирующие работу компьютера или ломающие всю систему. Главной тенденцией мирового хакерства стало его сращивание с преступными группировками. Хакеры стали более организованными, их техническое обеспечение иногда гораздо лучше, чем у правоохранительных органов. И самое главное теперь основной целью компьютерных гениев становится финансовая выгода. Активное внедрение IP-технологий во все сферы нашей жизни уже перестало всех удивлять, wi-fi в трамваях обычное дело. Не обошла эта тенденция и банковскую сферу, благодаря чему теперь управлять своими счетами посредством любого гаджета с интернетом можно из любой точки земного шара. А так как для доступа к финансовым операциям применяется двухфакторная идентификация «логин-пароль» за ней и устраивают охоту хакеры и мошенники. Другой стороной являются вирусы-вымагатели, с требованием вознаграждения за антивирусный код. Основные типы вредоносных ПО Не будем отвлекать внимание читателя на энциклопедические классификации вирусов, их предостаточно, и найти не составит труда, хотя постоянное появление новых видов делает любые градации неполными.

Рассмотрим основные типы вредоносных программ, их под одну гребенку и называют вирусами.

1. Трояны (троянец, троянский конь) – специально созданная программа распространяемая злоумышленниками и выполняющая конкретные задачи. Среди них кража информации, уничтожение данных, передача информации о пользователе третьим лицам и многое другое. Трояны могут быть созданы специально для распространения вирусов.
2. Вирус – самораспространяющаяся программа многократно себя копирующая и нарушающая работоспособность аппаратно-программного комплекса (ПК). Для распространения они должны прикрепиться к какой-либо программе. Современные вирусы могут быть полиморфными, т. е. изменять свой код, маскироваться.
3. Сетевые черви – программа, автоматически распространяющаяся в сети для выполнения определенных задач. Применяется для спам-рассылки и других вредоносных действий.
4. Руткит – программа, созданная для распространения другого вредоносного ПО.
5. Шпионское ПО – набор программ ориентированных на передачу данных о пользователе. Более четко определить существующие вредоносные программы очень проблематично и для неспециалиста не очень и нужно.

Гораздо важнее знать действие этих программ и способы защиты от них.

Преступная деятельность

Для обычных пользователей будет важнее знать, что все перечисленные выше программы применяются в комплексе и служат для различных неправомерных действий. Это может быть: Фарминг - это скрытые действия с host-файлом браузера, для того чтобы направить пользователя на необходимый фальшивый сайт Фишинг – определение личной информации пользователя при нахождении его в сети интернет (вот когда страдает

интернет-банкинг). Это может быть как электронное письмо с просьбой о передаче личных данных, так и скрытый вирус, самостоятельно пересылающий информацию. Именно так передаются пин-коды, пароли и т.д. Реклама – вредоносные программы используются для принудительного просмотра рекламных листовок или переадресации на определенные сайты.

В результате таких действий может произойти:

1. Кража аккаунта различных служб – электронная почта или любой другой сервис. У меня было на ETXT – бирже копирайтинга – взлом, переведены средства на другой аккаунт и просто куплены статьи. Было много раз у игроков онлайн-игр – продавались танки, самолеты, имущество героев и многое другое.

2. Кража аккаунтов платёжных систем (Вебмани, Яндекс), ну тут все понятно.

3. Блокировка компьютера, шифрование файлов пользователя для осуществления шантажа и вымогательства денег. Знакомые многим баннеры от лица МВД или службы безопасности страны.

Учтите, выплата средств не поможет разблокировке,

сделайте обычный откат системы или запустите диск с антивирусом, пригласите специалиста.

4. Перенаправление телефонного модема на дорогостоящие соединения.

5. Распространение платного ПО, имитирующего полезные программы.

В этой части хочется добавить, что не стоит рассчитывать только на компьютерное вмешательство. Мошенники отлично используют все персональные данные. Причем действуют комплексно и организованными группами, где распределены роли и есть не только человек, сидящий за компьютером.

Расследование таких преступлений большая головная боль для правоохранительных органов.

1. Самый «любимый» «лохотрон» нашей страны – полуночный звонок о сыне/дочке, попавшем в милицию и срочных деньгах для решения проблем. Знают и в каком человек городе, и что есть дети (хотя это не всегда важно, спросонок не все вспоминают, что бездетные).

2. Другой вариант, набирающий обороты, - при покупке/продаже товаров через интернет используются данные пользователя, осуществляется звонок от лица банка и потерпевший практически дает доступ к своему счету. Суммы снимаются с кредитных карт, потому могут быт гораздо больше, чем остатки на основных счетах. Таким способом обходят даже телефонную идентификацию посредством SMS-сообщений.

3. Закономерность, выявленная британскими учеными. Квартирные воры внимательно изучают аккаунты в соцсетях и могут свободно ориентироваться по жилью пользователей, выясняют, где расположены ценные вещи и многое другое. Любите писать в своем статусе: «Я в отпуске на Мальдивах»? Дописывайте тогда, где лежат ключи и деньги. Продолжать список можно довольно долго, мошеннических схем много, они разнообразны и всегда будут обновляться, так что лучше защититься.

Что же можно сделать?

1. Противопоставляем злому компьютерному гению … гений добрый. Над антивирусным ПО работает большой коллектив специалистов, так что установить его необходимо. Но еще им нужно и пользоваться. Проводите периодически полные проверки, вовремя обновляйте базы данных – это еще одно свидетельство противостояния в области вирусов. Обращайте внимание на работу ПК, сбои неполадки могут говорить о наличии вирусов.

2. Установите современную ОС. Они всегда делают запрос при внесении изменений.

3.Используйте проактивную защиту, не допускающую проникновения вирусов.

4. Работайте в учетных записях с правами пользователя. Тогда большинство вирусов просто не смогут установиться.

5. Используйте проверенные носители (флешки, CD-диски) и осуществляйте их проверку при запуске.

6. Пускайте к своему ПК только проверенных лиц.

7. Не открывайте файлы, полученные из ненадежных источников. Если не разбираетесь, то подучитесь азам информатики. Файл с музыкой не может иметь окончание .exe – это расширение исполняемых файлов. Если везде программа «весит» несколько гигабайт и платная, а вдруг есть возможность закачать, но размер ее всего несколько килобайт это точно вредоносный файл. И таких примеров много. Скачать вирус очень просто.

Неудивительно, что преступления в сфере компьютерных технологий находят своих «клиентов», ведь тут заняты целые коллективы людей. Потому будьте внимательны, устанавливайте антивирус и анализируйте свои действия. Тогда на виртуальный крючок вы точно не попадетесь

Источник: http://comp.web-3.ru/virus/?act=full&id_article=15328
© Портал Web-3.Ru

3.Компьютерные преступления и их виды

Для понимания масштабов объёма информатизации общества приведём такие цифры: в настоящий момент в мире насчитывается около 3,5 млрд людей, имеющих доступ к Интернету. Это половина всего населения Земли.

Сетью Интернет в совокупности со своими внутренними информационными сетями пользуются все банки и корпорации, аккумулирующие на своих счетах крупные денежные средства, лакомый кусок для разного рода компьютерных мошенников. Число преступных посягательств на имущество, совершаемых путём злоупотребления доверием или обманом, продолжает расти. В качестве статистических данных приведём отчёт Центра статистической информации Главного информационно-аналитического центра МВД России: в Российской Федерации за 2015 год было зарегистрировано 196700 преступлений, ответственность за которые предусмотрена статьями 159.1 - 159.6 УК РФ (по сравнению с прошедшим годом, это больше на 25 процентов, в 2014 году было зарегистрировано 160214 подобных преступлений). При этом небывалыми темпами растёт число мошенничеств в сфере компьютерной информации (995 зарегистрированных преступлений в 2014 году против 5443 в 2015 году). Раскрываемость же подобных деяний оставляет желать лучшего: в 2015 году она находилась на уровне 7,4 %. По итогам четырёх месяцев 2016 года негативная тенденция остаётся: зарегистрировано 1789 мошенничеств в сфере компьютерной информации (на 143,7% больше). В числе лидеров по количеству данных преступлений: Тюменская область (333 зарегистрированных преступления), Удмуртия (298), Республика Коми (223) . Раскрыто всего 72 преступления (на 5,3% меньше по сравнению с аналогичным периодом 2015 года). Низкая раскрываемость данного вида преступлений обусловлена достаточно высоким уровнем подготовки злоумышленников. Обычно они имеют как профессиональное образование, так и необходимую техническую аппаратуру, существенно облегчающую сокрытие следов при совершении компьютерных мошенничеств.

Увеличение числа киберпреступлений объясняют рост потребности владельцев информационных ресурсов (предприятий, организаций, государственных ведомств) в реализации систематических, всеобъемлющих мер по обеспечению информационной безопасности. Все негативные воздействия на объекты информационной безопасности можно разделить на три вида: нарушение конфиденциальности информации; разрушение (утеря, необратимое изменение) информации; недоступность информационных ресурсов - возникновение ситуаций, когда пользователи (все или их часть) на некоторый период времени теряют возможность доступа к необходимым данным (или информационным системам)[37].

На практике основными наиболее распространенными способами нарушения информационной безопасности являются: получение несанкционированного доступа к личной и конфиденциальной информации и их модификация, несанкционированное использование информационных ресурсов с целью получения выгоды или нанесения ущерба, кража электронных денег, осуществление атак типа «отказ в обслуживании» - распространение вирусов и других вредоносных программ, осуществляющих различные негативные воздействия.

В последнее время все больше внимания в прессе уделяется так называемым «компьютерным преступлениям». Такое внимание не беспочвенно. Дело в том, что сегодня практически ничего не делается без участия компьютеров в сфере коммуникаций, торговли, банковских и биржевых операций и многого другого. Все важнейшие информационные функции современного общества, так или иначе «завязаны» на компьютерах, компьютерных сетях и компьютерной информации.

С появлением современных средств вычислительной техники и телекоммуникаций традиционные преступления – воровство, мошенничество, шпионаж, вымогательство трансформировались в новые формы. Кроме того, появились специфические для компьютерных систем и сетей преступления. Намечается тенденция к использованию информационных технологий организованными преступными группами и распространение их деятельности на межгосударственный уровень. Сотрудники правоохранительных органов при раскрытии и расследовании компьютерных преступлений неизбежно сталкиваются с большими трудностями, так как преступления в сфере компьютерной обработки информации характеризуются высокой скрытностью, трудностями сбора улик по установлению фактов их совершения, сложностью доказывания в суде. Субъекты преступлений – это, как правило, высококвалифицированные программисты, инженеры, специалисты в области телекоммуникационных систем, банковские работники, бывшие сотрудники спецслужб.

Понятие *«компьютерная преступность”* охватывает преступления, совершаемые с помощью компьютеров, информационно вычислительных систем и средств телекоммуникаций, или направленные против них с корыстными либо некоторыми другими целями.

Компьютерное преступление как уголовно-правовое понятие- это предусмотренное уголовным законом умышленное нарушение чужих прав и интересов в отношении автоматизированных систем обработки данных, совершенное во вред подлежащим правовой охране правам и интересам физических и юридических лиц, общества и государства.

Отечественные и зарубежные издания и средства массовой информации последних лет наводнены различными понятиями, обозначающими те или иные новые проявления

криминального характера в информационной области. Встречаются наименования и «компьютерные преступления», «коммуникационные преступления», и «кибербандитизм». Преступников именуют «хакеры», «кракеры», «киберпанки», «бандиты на информационных супермагистралях». Различие в терминологии указывает не только на обеспокоенность общества новой угрозой, но и на отсутствие полного понимания сути этой угрозы.

Для компьютерных преступлений характерны следующие особенности:

- высокая латентность компьютерных преступлений, раскрывается лишь 1-3% из их числа;
- сложность сбора доказательств и процесса доказывания в суде;
- отсутствие четкой программы борьбы с компьютерными преступлениями (одна из причин того, что примерно 90% преступлений данной категории выявляется благодаря случайностям;
- сложность самого процесса раскрытия (в узком смысле слова) компьютерных преступлений;
- отсутствие достаточной следственной практики по расследованию компьютерных преступлений в Российской Федерации.

В более общем виде способы совершения КП можно классифицировать на:

- несанкционированный доступ;
- вирусная модификация;
- перехват информации;
- комбинированное использование.

Несанкционированный доступ включает:

- несанкционированное подключение;
- несанкционированную модификацию;
- несанкционированное блокирование;
- несанкционированное уничтожение.

К несанкционированному подключению относятся – несанкционированный доступ к вычислительным ресурсам, воздействие на парольно-ключевые системы, установка программных и закладных устройств.

При совершении криминальных действий, связанных с несанкционированным копированием информации, преступники, как правило, копируют:

- документы, содержащие интересующую их информацию;
- технические носители;
- информацию, обрабатываемую в информационных системах.

Под модификацией информации понимается внесение в нее любых изменений, обусловливающих ее отличие от той, которую собственник информационного ресурса включил в систему и которой владеет.

Несанкционированное блокирование информации заключается в невозможности доступа к ней со стороны законного пользователя.

Уничтожение информации включает и полную или частичную ликвидацию, как самой информации, так и ее носителей.

Под *перехватом* понимают получение разведывательной информации путем приема электромагнитного и акустического излучения пассивными средствами приема, расположенными, как правило, на безопасном расстоянии от источника информации.

К наиболее типичным способам совершения компьютерных преступлений специалисты относят следующие:

- подделка отчетов и платежных ведомостей;
- приписка сверхурочных часов работы;
- фальсификация платежных документов;
- хищение из денежных фондов;
- добывание запасных частей и редких материалов;
- кража машинного времени;
- вторичное получение уже произведенных выплат;
- фиктивное продвижение по службе;
- получение фальшивых документов;
- внесение изменений в программы и машинную информацию;
- перечисление денег на фиктивные счета;
- совершение покупок с фиктивной оплатой и др.

В своих преступных деяниях компьютерные преступники руководствуются следующими основными мотивами:

а) выйти из финансовых затруднений;

б) получить, пока не поздно, от общества то, что оно якобы задолжало преступнику;

в) отомстить фирме и работодателю;

г) выразить себя, проявить свое «я»;

д) доказать свое превосходство над компьютерами.

Отличительными особенностями данных преступлений являются высокая латентность, сложность сбора доказательств, транснациональный характер (как правило, с использованием телекоммуникационных систем), значительность материального ущерба, а также специфичность самих преступников. Как правило, ими являются высококвалифицированные программисты, банковские служащие.

Высокая латентность компьютерных преступлений обусловлена тем, что многие организации разрешают конфликт своими силами, поскольку убытки от расследования могут оказаться выше суммы причиненного ущерба (изъятие файлового сервера для проведения экспертизы может привести к остановке работы на срок до двух месяцев, что неприемлемо ни для одной организации). Их руководители опасаются подрыва своего авторитета в деловых кругах и в результате – потери большого числа клиентов, раскрытия в ходе судебного разбирательства системы безопасности организации, выявления собственной незаконной деятельности.

Непосредственным предметом преступного посягательства по делам о КП являются следующие:

- компьютерная система (ЭВМ, сервер, рабочая станция);
- процесс обработки и хранения информации;
- компьютерные сети (сети ЭВМ).

Нарушение целостности информации без непосредственного участия человека включает:

- выход из строя серверов, рабочих станций;
- сбои в сети электропитания;
- выход из строя носителей информации;
- неполадки в кабельной системе, сетевом оборудовании;

- прочие аппаратные и программные сбои.

Российские исследователи отмечают следующие особенности совершения компьютерных преступлений в финансовой сфере:

- большинство злоумышленников – клерки, хотя высший персонал банка также может совершить преступление и нанести банку гораздо больший ущерб, однако такого рода случаи происходят намного реже;
- как правило, злоумышленники используют свои собственные счета, на которые переводятся похищенные суммы;
- большинство преступников не знает, как «отмыть» украденные деньги; умение совершить преступление и умение получить деньги – это не одно и тоже;
- компьютерные преступления не всегда высоко технологичны, ряд злоумышленных действий достаточно просто может быть совершен обслуживающим персоналом;
- многие злоумышленники объясняют свои действия тем, что они всего лишь берут в долг у банка с последующим возвратом; как правило, этого не происходит.

В зависимости от способа воздействия на компьютерную систему специалисты выделяют четыре вида компьютерных преступлений:

- *Физические злоупотребления,* которые включают в себя разрушение оборудования; уничтожение данных или программ; ввод ложных данных, кражу информации, записанной на различных носителях.
- *Операционные злоупотребления,* представляющие собой: мошенничество (выдача себя за другое лицо или использование прав другого лица); несанкционированное использование различных устройств.
- *Программные злоупотребления,* которые включают в себя: различные способы изменения системы математического обеспечения («логическая бомба»– введение в программу команды компьютеру проделать в определенный момент какое-либо несанкционированное действие; «троянский конь»– включение в обычную программу своего задания).
- *Электронные злоупотребления,* которые включают в себя схемные и аппаратные изменения, приводящие к тому же результату, что и изменение программы.

Все способы совершения компьютерных преступлений можно объединить в три основные группы: методы перехвата, методы несанкционированного доступа и методы манипуляции.

- *Методы перехвата.*

Непосредственный перехват – осуществляется либо прямо через внешние коммуникационные каналы системы, либо путем непосредственного подключения к линиям периферийных устройств. При этом объектами непосредственного подслушивания являются кабельные и проводные системы, наземные микроволновые системы, системы спутниковой связи, а также специальные системы правительственной связи.

Электромагнитный перехват. Перехват информации осуществляется за счет излучения центрального процессора, дисплея, коммуникационных каналов, принтера и т.д. Может осуществляться преступником, находящимся на достаточном удалении от объекта перехвата.

- Методы несанкционированного доступа.

Стоит обратить внимание на то, что существует множество программ-«взломщиков», называемых на профессиональном языке HACK-TOOLS(инструмент взлома). Эти программы работают по принципу простого перебора символов. Но они становятся малоэффективными в компьютерных системах, обладающих программой-«сторожем» компьютерных портов, ведущей автоматический протокол обращений к компьютеру и отключающей абонента, если пароль не верен. Поэтому в последнее время преступниками стал активно использоваться метод «интеллектуального перебора», основанный на подборе предполагаемого пароля, исходя из заранее определенных тематических групп его принадлежности. Интересны результаты экспериментов, представленные специалистами в форме таблицы (табл. 2) [58].

Таблица 2

	Тематические группы паролей	% частоты выбора пароля человеком	% раскрываемости пароля
	Имена, фамилии и производные	22,2	54,5
	Интересы (хобби, спорт, музыка)	9,5	29,2
	Даты рождения, знаки зодиака свои и близких; их комбинация с первой группой	11,8	54,5
	Адрес жительства, место рождения	4,7	55,0
	Номера телефонов	3,5	66,6
	Последовательность клавиш ПК, повтор символа	16,1	72,3
	Номера документов (паспорт, пропуск, удостоверение и т.д.)	3,5	100,0
	Прочие	30,7	5,7

«Неспешный выбор». Отличительной особенностью данного способа совершения преступления является то, что преступник осуществляет несанкционированный доступ к компьютерной системе путем нахождения слабых мест в ее защите. Однажды обнаружив их, он может, не спеша исследовать содержащуюся в системе информацию, скопировать ее на свой физический носитель и, возвращаясь к ней много раз, выбрать наиболее оптимальный предмет посягательства. Обычно такой способ используется преступником в отношении тех, кто не уделяет должного внимания регламенту проверки своей системы, предусмотренной методикой защиты компьютерной системы.

«Брешь». В отличие от «неспешного выбора», при данном способе преступником осуществляется конкретизация уязвимых мест в защите: определяются участки, имеющие ошибку или неудачную логику программного строения. Выявленные таким образом «бреши» могут использоваться преступником многократно, пока не будут обнаружены. Появление этого способа обусловлено тем, что программисты иногда допускают ошибки при разработке программных средств, которые не всегда удается обнаружить в процессе отладки программного продукта. Например, методика качественного программирования предполагает: когда программа X требует использования программы V – должна выдаваться только информация, необходимая для вызова V, а не она сама. Для этих целей применяются программы группировки данных. Составление последних является довольно скучным и утомительным, поэтому программисты иногда сознательно нарушают методику программирования и делают различные упрощения, указывая, например, индекс места нахождения нужных данных в рамках более общего списка команд программы. Именно это и создаст возможности для последующего нахождения подобных «брешей».

«Люк». Данный способ является логическим продолжением предыдущего. В этом случае в найденной «бреши» программа разрывается и туда дополнительно преступник вводит одну или несколько команд. Такой «люк» открывается по мере необходимости, а включенные команды автоматически выполняются.

Следует обратить внимание на то, что при этом всегда преступником осуществляется преднамеренная модификация (изменение) определенной компьютерной информации.

«Маскарад». Данный способ состоит в том, что преступник проникает в компьютерную систему, выдавая себя за законного пользователя. Система защиты средств компьютерной техники, которые не обладают функциями аутентичной идентификации пользователя (например, по биометрическим параметрам: отпечаткам пальцев, рисунку сетчатки глаза, голосу и т.п.) оказываются не защищенными от этого способа. Самый простейший путь к проникновению в такие системы – получить коды и другие идентифицирующие шифры законных пользователей. Это можно сделать посредством приобретения списка пользователей со всей необходимой информацией путем подкупа, коррумпирования, вымогательства или иных противоправных деяний в отношении лиц, имеющих доступ к указанному документу; обнаружения такого документа в организациях, где не налажен должный контроль за их хранением; отбора информации из канала связи и т.д. Так, например, задержанный в декабре 1995 года сотрудниками московского РУОПа преступник похищал наличные денежные средства из банкоматов банка «Столичный» с использованием обычной электронной кредитной карточки путем подбора цифровой комбинации кода доступа в компьютерную систему управления счетами клиентов банка. Общая сумма хищения составила 400 млн. руб.

«Аварийный». В этом способе преступником используется тот факт, что в любом компьютерном центре имеется особая программа, применяемая как системный инструмент в случае возникновения сбоев или других отклонений в работе ЭВМ (аварийный или контрольный отладчик). Принцип работы данной программы заключается в том, что она позволяет достаточно быстро обойти все имеющиеся средства защиты информации и компьютерной системы с целью получения аварийного доступа к наиболее ценным данным. Такие программы являются универсальным «ключом» в руках преступника.

Особую опасность представляет несанкционированный доступ в компьютерные системы финансовых учреждений с целью хищения финансовых средств.

Методики несанкционированного доступа сводится к двум разновидностям:

«Взлом» изнутри: преступник имеет физический доступ к терминалу, с которого доступна интересующая его информация и может определенное время работать на нем без постороннего контроля.

«Взлом» извне: преступник не имеет непосредственного доступа к компьютерной системе, но имеет возможность каким-либо способом (обычно посредством удаленного доступа через сети) проникнуть в защищенную систему для внедрения специальных программ, произведения манипуляций с обрабатываемой или хранящейся в системе информацией, или осуществления других противозаконных действий.

Отмечается тенденция к переходу от разовых преступлений по проникновению в системы со своих или соседних рабочих мест к совершению сетевых компьютерных преступлений путем «взлома» защитных систем организаций.

Хищение информации. Правонарушения, связанные с хищением информации, могут принимать различные формы в зависимости от характера системы, в отношении которой осуществляется несанкционированный доступ. Информация, являющаяся объектом преступного посягательства, может быть отнесена к одному из четырех типов:

- персональные данные;
- корпоративная информация, составляющая коммерческую тайну;
- объекты интеллектуальной собственности и материалы, защищенные авторским правом;
- глобальная информация, имеющая значение для развития отраслей промышленности, экономики отдельных регионов и государств.

Похищаются сведения о новейших научно-технических разработках, планах компании по маркетингу своей продукции и заключаемых сделках.

Типичным злоупотреблением, посягающим на объекты авторских прав, являются преступления, связанные с несанкционированным размножением компьютерных программ.

Предметом хищения может быть также другая экономически важная информация, в частности, реквизиты банковских счетов и номера кредитных карточек.

Уивинг – одно из наиболее распространенных преступлений этого вида, связанное с кражей услуг, происходит в процессе «запутывания следов». Злоумышленник проходит через многочисленные системы и многочисленные телекоммуникационные сети – Интернет, системы сотовой и наземной телефонной связи, чтобы скрыть свое подлинное имя и местонахождение. При такой ситуации причиной проникновения в данный компьютер является намерение использовать его как средство для атаки на другие системы.

Повреждение системы. Данная группа объединяет преступления, совершаемые с целью разрушить или изменить данные, являющиеся важными для владельца или многих пользователей системы – объекта несанкционированного доступа.

Использование вирусов. Применение данного средства повреждения компьютерных систем доступно в настоящее время не только профессиональным программистам, но и людям, обладающим лишь поверхностными познаниями в этой сфере. Во многом это обусловлено доступностью самих вредоносных программ и наличием простой технологии их создания.

Особую опасность представляют злоупотребления, связанные с распространением вирусов через Интернет.

Некоторые из таких нарушений связаны с компьютерами телефонных сетей.

«Троянский конь»- способ, состоящий в тайном введении в чужую программу таких команд, которые позволяют осуществлять иные, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность.

Действия такого рода часто совершаются сотрудниками, которые стремятся отомстить за несправедливое, по их мнению, отношение к себе, либо оказать воздействие на администрацию предприятия с корыстной целью.

«Логическая бомба»– тайное встраивание в программу набора команд, который должен сработать лишь однажды, но при определенных условиях.

«Временная бомба»– разновидность логической бомбы, которая срабатывает при достижении определенного момента времени.

«Моделирование» используется как для анализа процессов, в которые преступники хотят вмешаться, так и для планирования методов совершения преступления.

Типологизация компьютерных преступников представлена на рис.6.

Рис. 6. Субъекты компьютерных преступлений

Лица, совершающие компьютерные преступления, могут быть объединены в три большие группы:

- лица, не связанные трудовыми отношениями с организацией жертвой, но имеющие некоторые связи с ней;
- сотрудники организации, занимающие ответственные посты;
- сотрудники-пользователи ЭВМ, злоупотребляющие своим положением.

Например, *около 90% злоупотреблений в финансовой сфере, связанных с нарушениями в области информационной безопасности, происходит при прямом или косвенном участии действующих или бывших работников банков.* При этом на преступный путь часто становятся самые квалифицированные, обладающие максимальными правами в автоматизированных системах категории банковских служащих – системные администраторы и другие сотрудники служб автоматизации банков.

По сведениям Национального центра данных о преступности, связанной с ЭВМ (Лос-Анджелес, США), компьютерные правонарушения наиболее часто совершаются программистами, студентами и операторами ввода исходных данных. В табл. 3 указаны основные типы и субъекты угроз для компьютерных систем.

Таблица 3

Типы и субъекты угроз

Тип угроз	Оператор	Руково-дитель	Прог раммист	Инженер (техник)	Пользо-ватель	Конкурент
Изменение кодов	+		+			
Копирование файлов	+		+			
Уничтожение файлов	+	+	+		+	+
Присвоение программ			+	+		+
Шпионаж	+	+	+			+
Установка			+	+		+
Саботаж	+		+	+		+
Продажа данных	+	+	+		+	
Воровство		+	+		+	+

Субъектов компьютерных преступлений с точки зрения профессиональной подготовленности принято подразделять на лиц, совершающих преступления:

а) «нетехнические»;

б) «технические», требующие минимума специальных знаний;

в) «высокотехнические», возможные при условии основательного владения вычислительной техникой.

Практика показывает, что большинство преступлений категории «а» совершают малознакомые с вычислительной техникой служащие со средним образованием. Однако этих людей отличают два качества: они имеют доступ к компьютеру и знают, какие функции выполняет он в их организации. «Нетехнические» преступления совершаются главным образом путем кражи пароля доступа к файлам информации, хранящейся в машинной памяти. Владея паролем и определенными навыками, можно войти в засекреченные файлы, изменить их содержание и т.п. Эти преступления довольно просты для расследования, и, усилив защиту системы, их легко предупредить.

«Технические» преступления связаны с манипуляциями программами, которые составлены специалистами. Изменить их могут лишь лица, имеющие соответствующую квалификацию. Наибольшую трудность для правоохранительных органов представляют «высокотехнические» преступления.

Анализируя компьютерные преступления, можно установить общность «почерка» злоумышленника (или организованной группы):

- реализуется несанкционированный доступ к автоматизированной информационной системе, к ее аппаратно-программным средствам, модифицируются важные записи;
- вносятся изменения в существующее программное обеспечение для создания специальных счетов физических и юридических лиц, рассылки фальшивых платежных документов и пр.
- параллельно уничтожаются следы компьютерного преступления путем модернизации бухгалтерских документов аналитического и синтетического учета;
- осуществляется получение наличных средств.

Опасность, как правило, таится внутри организации, а не вне ее. Компьютерному преступлению способствуют такие предпосылки, как отсутствие надлежащей системы бухгалтерского учета, комплексной защиты информации и ее контроля, слабая готовность персонала, отсутствие или слабая организация системы разделения доступа и т.п.

Причинами, побуждающими недобросовестных сотрудников к совершению компьютерных преступлений, являются:

- корысть;
- ошибка пользователей и программистов неумышленного характера;

безответственность в организации системы информационной безопасности;

- самоутверждение путем демонстрации своего превосходства;
- месть за какие-либо действия администрации;
- недостатки созданных информационных систем и технологий.

Полагается, что преступления в сфере компьютерной информации являются

«беловоротничковыми преступлениями» («БП»– это такие правонарушения, при совершении которых имеет место нанесение ущерба торговле, нарушение страховых и валютных правил, взяточничество и т.п.). В отличии от многих других «беловоротничковых преступлений», которые в большинстве случаев совершаются, несмотря на существующую систему учета и контроля, компьютерные преступления обычно являются следствием отсутствия надлежащего контроля. Ранее компьютер считали защищенным от всякого рода «злоумышленников», и поэтому различные предосторожности рассматривались излишними.

Общей причиной существования преступности является несовершенство человека, его предрасположенность, как к добру, так и злу.

По мнению специалистов, большинство серьезных компьютерных преступлений, связанных с неправомерным доступом к компьютерной информации, совершаются группой лиц. Это подтверждается и статистикой. Так, 38% преступников действовали без соучастников, тогда как 62% - в составе преступных групп.

Прежде всего, это связано с тем, что на современном этапе развития компьютерных технологий одному человеку практически невозможно одновременно нейтрализовать системы защиты, выполнить какие-либо манипуляции с информацией, а затем еще запутать за собой следы преступления.

В последнее время участились случаи воздействия на вычислительную систему при помощи специально созданных программ. Под вредоносными программами в дальнейшем будем понимать такие программы, которые прямо или косвенно дезорганизуют процесс обработки информации или способствуют утечке или искажению информации.

Ниже рассмотрим некоторые (самые распространенные) виды подобных программ:

«Троянский конь» - программа, выполняющая в дополнение к основным (проектным и документированным) не описанные в документации действия. Аналогия с древнегреческим «троянским конем» таким образом, вполне оправдана – в не вызывающей подозрений оболочке таится угроза.

Опасность «троянского коня» заключается в дополнительном блоке команд, тем или иным образом вставленном в исходную безвредную программу, которая затем предлагается (дарится, продается, подменяется) пользователем. Этот блок команд может срабатывать при наступлении некоторого условия (даты, времени и т.д., либо по команде извне).

Наиболее опасные действия «троянский конь» может выполнять, если запустивший ее пользователь обладает расширенным набором привилегий. В этом случае злоумышленник, составивший и внедривший «троянского коня», и сам этими привилегиями не обладающий, может выполнить несанкционированные привилегированные функции чужими руками. Или, например, злоумышленника очень

интересуют наборы данных пользователя, запустившего такую программу. Последний может даже не обладать расширенным набором привилегий – это не помешает выполнению несанкционированных действий.

Вирус– это программа, которая может заражать другие программы путем включения в них своей, возможно модифицированной, копии, причем последняя сохраняет способность к дальнейшему размножению.

Своим названием компьютерные вирусы обязаны определенному сходству с вирусами биологическими:

- способностями к саморазмножению;
- высокой скорости распространения;
- избирательности поражаемых систем (каждый вирус поражает только определенные системы или однородные группы систем);
- наличию в большинстве случаев определенного инкубационного периода;
- способности «заражать» еще незараженные системы;
- трудности борьбы с вирусами и т.д.

История компьютерных вирусов представлена на рис.7.

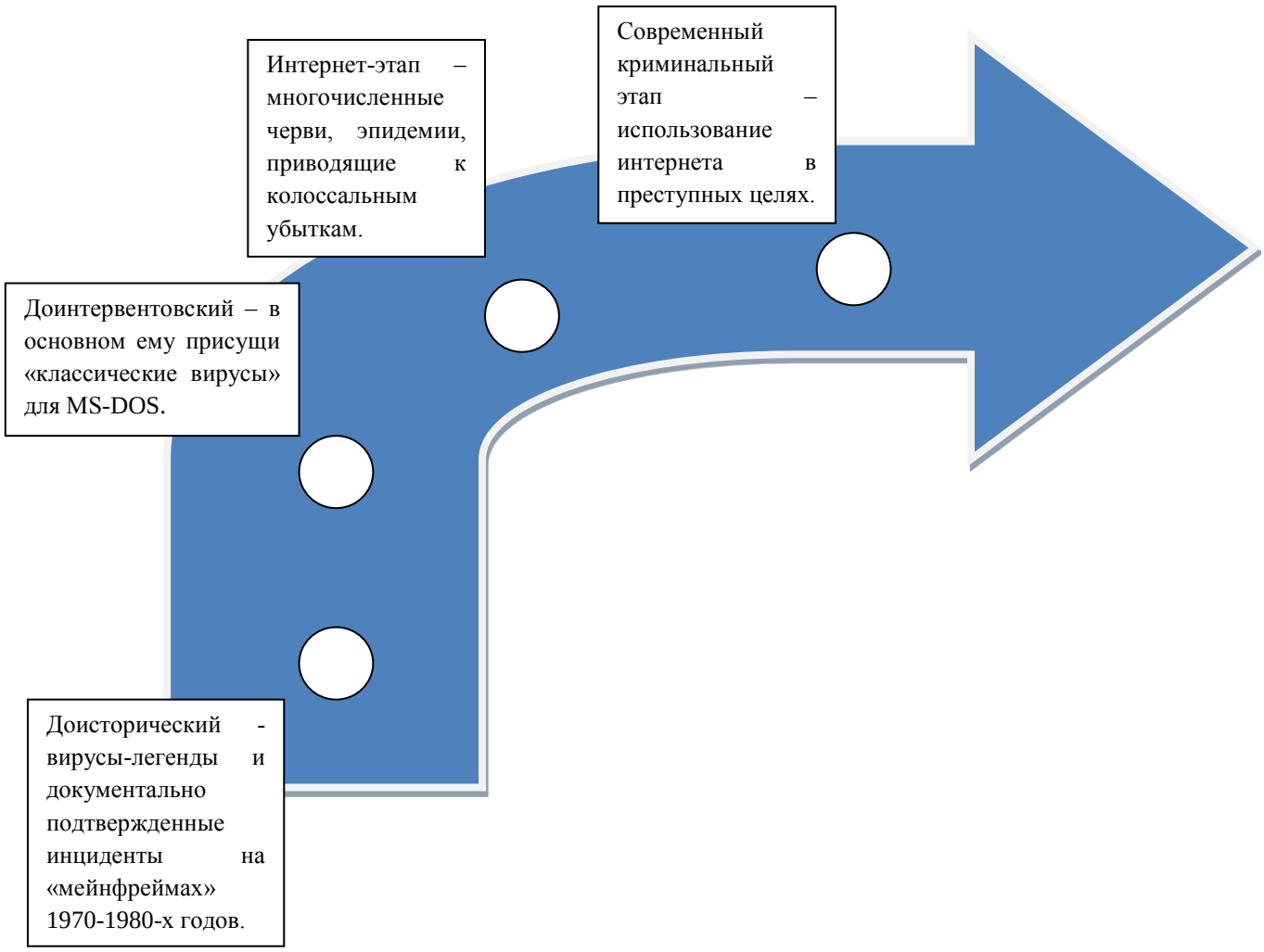


Рис. 7. История компьютерных вирусов.

Классификация способов несанкционированного копирования представлены на рис.8.

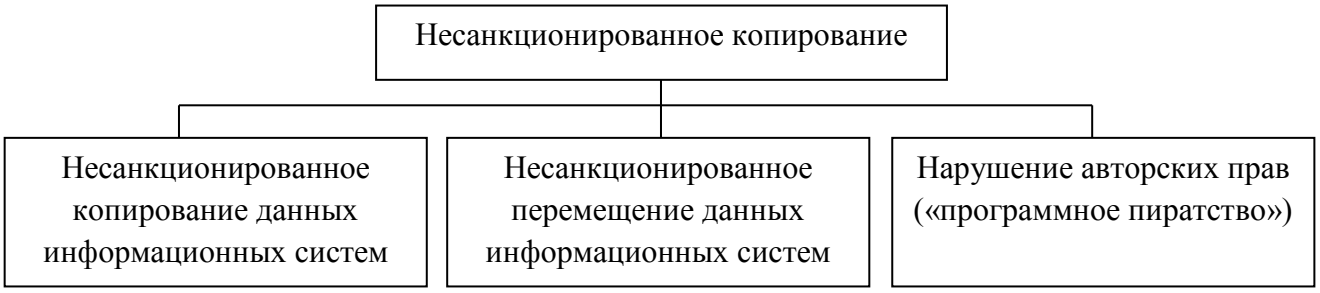


Рис. 8. Несанкционированное копирование информации

В последнее время к этим особенностям, характерным для вирусов компьютерных, можно добавить еще и постоянно увеличивающуюся быстроту появления модификаций и новых поколений вирусов, что можно объяснить идеями злоумышленников определенного склада ума.

Программа, внутри которой находится вирус, называется «зараженной». Когда такая программа начинает работу, то сначала управление получает вирус. Вирус находит и «заражает» другие программы, а также выполняет какие-нибудь вредные действия.

Процесс заражения вирусом программных файлов можно представить следующим образом. В зараженной программе код последней изменяется таким образом, чтобы вирус получил управление первым, до начала работы программы – вирусоносителя. При передаче управления вирусу он каким-либо способом находит новую программу и выполняет вставку собственной копии в начало или добавление ее в конец этой, обычно еще не зараженной, программы. Если вирус записывается в конец программы, то он корректирует код программы с тем, чтобы получить управление первым. После этого управление передается программе-вирусоносителю, и та нормально выполняет свои функции. Более изощренные вирусы могут для получения управления изменять системные области накопителя (например, сектор каталога), оставляя длину и содержимое заражаемого файла без изменений.

Макровирусы. Эта особая разновидность вирусов поражает документы, выполненные в некоторых прикладных программах, имеющих средства для исполнения так называемых макрокоманд.

В частности, к таким документам относятся документы текстового процессора MicrosoftWord. Заражение происходит при открытии файла документа в окне программы, если в ней не отключена возможность исполнения макрокоманд.

«Червь» - программа, распространяющаяся через сеть и не оставляющая своей копии на магнитном носителе. «Червь» использует механизмы поддержки сети для определения узла, который может быть заражен. Затем с помощью тех же механизмов передает свое тело или его часть на этот узел и либо активизируется, либо ждет для этого подходящих условий.

Наиболее известный представитель этого класса – вирус Морриса (или, вернее, «червь Морриса»), поразивший сеть Internet в 1988 г. Наиболее подходящей средой распространения «червя» является сеть, все пользователи которой считаются дружественными и доверяют друг другу. Отсутствие защитных механизмов как нельзя лучше способствует уязвимости сети.

«Жадные» программы– это программы, которые при выполнении стремятся монополизировать какой-либо ресурс системы, не давая другим программам возможности использовать его. Доступ таких программ к ресурсам системы обычно приводит к нарушению ее доступности. Естественно, такая атака будет активным вмешательством в работу системы. Непосредственной атаке обычно подвергаются ключевые объекты системы: процессор, оперативная память, устройства ввода-вывода.

Тупиковая ситуация возникает, когда «жадная» программа бесконечна (например, исполняет заведомо бесконечный цикл). Однако во многих операционных системах существует возможность ограничения времени процессора, используемого задачей. Это не относится к операциям, выполняющимся в зависимости от других программ, например, к операциям ввода-вывода, которые завершаются асинхронно к основной программе; время их выполнения не включается в счет времени программы. Перехватывая сообщение о завершении операции ввода-вывода и посылая вновь запрос на новый ввод-вывод, можно добиться по-настоящему бесконечной программы.

Другой пример «жадной» программы – программа, захватывающая слишком большую область оперативной памяти. В оперативной памяти последовательно размещаются данные, например подкачиваемые с внешнего носителя. В конце концов память может оказаться во владении одной программы, и выполнение других окажется невозможным.

Шпионские программы предназначены для сбора данных и отправки их третьей стороне без вашего ведома и согласия. Такие программы могут отслеживать нажатия клавиш (клавиатурные шпионы), собирать конфиденциальную информацию (пароли, номера кредитных карт, PIN-коды и т.д.), отслеживать адреса электронной почты в почтовом ящике или особенности вашей работы в Интернете. Кроме того, шпионские программы неизбежно снижают производительность компьютера.

Захватчики паролей. Это программы специально предназначены для воровства паролей. При попытке входа имитируется ввод имени и пароля, которые пересылаются владельцу программы-захватчика, после чего выводится сообщение об ошибке ввода и управление возвращается операционной системе. Пользователь, думающий, что допустил ошибку при наборе пароля, повторяет вход и получает доступ к системе. Однако его имя и пароль уже известны владельцу программы-захватчика. Перехват пароля может осуществляться и другим способом – с помощью воздействия на программу, управляющую входом пользователей в систему и ее наборы данных.

Методика воздействия вредоносных программ в значительной мере зависит от организации обработки информации в системе, разработанной политики безопасности, возможностей установленных средств защиты, а также добросовестности администратора и оператора. Для реализации НСД существует два способа:

-во-первых, можно преодолеть систему защиты, то есть путем различных воздействий на нее прекратить ее действия в отношении себя или своих программ. Это сложно, трудоемко и не всегда возможно, зато эффективно;

- во-вторых, можно понаблюдать за тем, что «плохо лежит», то есть какие наборы данных, представляющие интерес для злоумышленника, открыты для доступа по недосмотру или умыслу администратора. Такой доступ, хотя и с некоторой натяжкой, тоже можно назвать несанкционированным, его легко осуществить, но от него легко и защититься. К этому же типу относится НСД с подбором пароля, поскольку осуществить

такой подбор возможно лишь в случае нарушения правил составления паролей и использования в качестве пароля человеческих имен, повторяющихся символов и пр.

В подавляющем большинстве случаев НСД становится возможным из-за непродуманного выбора средств защиты, их некорректной установки и настройки, плохого контроля работы, а также при небрежном отношении к защите своих собственных данных.

Атаки «салями» более всего характерны для систем, обрабатывающих денежные счета и, следовательно, для банков особенно актуальны. Принцип атак «салями» построен на том факте, что при обработке счетов используются целые единицы (центы, рубли, копейки), а при исчислении процентов нередко получаются дробные суммы.

Например, 6,5% годовых от $102,87 за 31 день составит $0,5495726. Банковская система может округлить эту сумму до $0.55. Однако если пользователь имеет доступ к банковским счетам или программам их обработки, он может округлить ее в другую сторону – до $0.54, а разницу в 1 цент записать на свой счет. Владелец счета вряд ли ее заметит, а если и обратит внимание, то спишет ее на погрешности обработки и не придаст значения. Злоумышленник же получит прибыль в один цент, при обработке 10.000 счетов в день. Его прибыль таким образом составит $1000, т.е. около $300 000 в год.

Отсюда и происходит название таких атак – как колбаса салями изготавливается из небольших частей разных сортов мяса, так и счет злоумышленника пополняется за счет различных вкладчиков. Естественно, такие атаки имеют смысл лишь в тех организациях, где осуществляется не менее 5000 – 10000 транзакций в день, иначе не имеет смысла рисковать, поскольку в случае обнаружения преступника просто определить. Таким образом, атаки «салями» опасны в основном для крупных банков.

Причинами атак «салями» являются, во-первых, погрешности вычислений, позволяющие трактовать правила округления в ту или иную сторону, а во-вторых, огромные объемы вычислений, необходимые для обработки счетов. Успех таких атак зависит не столько от величины обрабатываемых сумм, сколько от количества счетов (для любого счета погрешность обработки одинакова). Атаки «салями» достаточно трудно распознаются, если только злоумышленник не начинает накапливать на одном счете миллионы.

«Маскарад»

Под «маскарадом» понимается выполнение каких-либо действий одним пользователем от имени другого пользователя. При этом такие действия другому пользователю могут быть разрешены. Нарушение заключается в присвоении прав и привилегий.

Цель «маскарада» - сокрытие каких-либо действий за именем другого пользователя или присвоение прав и привилегий другого пользователя для доступа к его наборам данных или для использования его привилегий.

«Маскарад» - это способ активного нарушения защиты системы, он является опосредованным воздействием, то есть воздействием, совершенным с использованием возможностей других пользователей.

Примером «маскарада» может служить вход в систему под именем и паролем другого пользователя, при этом система защиты не сможет распознать нарушение. В этом случае «маскараду» обычно предшествует взлом системы или перехват пароля.

Другой пример «маскарада» - присвоение имени другого пользователя в процессе работы. Это может быть сделано с помощью средств операционной системы (некоторые

операционные системы позволяют изменять идентификатор пользователя в процессе работы) или с помощью программы, которая в определенном месте может изменить определенные данные, в результате чего пользователь получит другое имя. В этом случае «маскараду» может предшествовать захват привилегий, или он может быть осуществлен с использованием какой-либо ошибки в системе.

«Маскарадом» также называют передачу сообщений в сети от имени другого пользователя. Способы замены идентификатора могут быть разные, обычно они определяются ошибками и особенностями сетевых протоколов. Тем не менее на приемном узле такое сообщение будет воспринято как корректное, что может привести к серьезным нарушениям работы сети. Особенно это касается управляющих сообщений, изменяющих конфигурацию сети, или сообщений, ведущих к выполнению привилегированных операций.

Наиболее опасен «маскарад» в банковских системах электронных платежей,где неправильная идентификация клиента может привести к огромным убыткам. Особенно это касается платежей с помощью электронных банковских карт. Сам по себе метод идентификации с помощью персонального идентификатора (PIN) достаточно надежен, нарушения могут происходить вследствие ошибок его использования. Это произойдет, например, в случае утери кредитной карты, при использовании очевидного идентификатора (своего имени, ключевого слова и т.д.). Поэтому клиентам надо строго соблюдать все рекомендации банка по выполнению такого рода платежей.

«Логической бомбой» называют участок программы, который реализует некоторые действия при наступлении определенных условий в дате или имени файла.

Мировая компьютерная общественность достаточно хорошо знакома с «логическими бомбами». Логическая бомба является одним из излюбленных способов мести программистов Компаниям, которые их уволили или чем-либо обидели. При этом чаще всего срабатывание бомбы становится в зависимость от установки в системе даты – так называемые «часовые» бомбы. Это очень удобно: допустим, программист знает, что его уволят 1 февраля. В таком случае он может установить «часовую» бомбу на взрыв, допустим 6 мая, когда сам он будет уже вне пределов досягаемости для пострадавшей компании.

После ее запуска на экране дисплея можно увидеть мультипликационные картинки с американской певицей Мадонной, причем показ завершается выдачей сообщения следующего содержания «Только идиот использует свой компьютер для того, чтобы рассматривать видеозвезд!». Во время демонстрации бомба удаляет себя, но заодно удаляет и все файлы на доступных для нее дисках.

Эксперты считают, что на сегодняшний день число существующих вирусов перевалило за 50 тысяч, причем ежедневно появляется от 6 до 9 новых. Реально циркулирующих вирусов в настоящее время насчитывается около более 200.

Один из авторитетнейших «вирусологов» страны Евгений Касперский предлагает условно классифицировать вирусы по следующим признакам:

- по среде обитания вируса;
- по способу заражения среды обитания;
- по деструктивным возможностям;
- по особенностям алгоритма вируса.

Более подробная классификация внутри этих групп представлена ниже.

Классификация компьютерных вирусов по среде обитания:

Сетевые	Распространяются по компьютерной сети
Файловые	Внедряются в выполняемые файлы
Загрузочные	Внедряются в загрузочный сектор диска (Boot-сектор)

Классификация компьютерных вирусов по способам заражения:

Резидентные	Находятся в памяти, активны до выключения компьютера
Нерезидентные	Не заражают память, являются активными ограниченное время
Безвредные	Практически не влияют на работу; уменьшают свободную память на диске в результате своего размножения
Неопасные	Уменьшают свободную память, создают звуковые, графические и прочие эффекты
Опасные	Могут привести к потере программ или системных данных
Очень опасные	Уменьшают свободную память, создают звуковые, графические и прочие эффекты

С учетом особенностей алгоритма вируса выделяют:

Вирусы-«спутники»	Вирусы, не изменяющие файлы, создают для EXE-файлов файлы-спутники с расширением .com
Вирусы-«черви»	Распространяются по сети, рассылают свои копии, вычисляя сетевые адреса
«паразитические»	Изменяют содержимое дисковых секторов или файлов
«стелс»-вирусы («невидимки»)	Перехватывают обращения операционной системы к пораженным файлам или секторам и подставляют вместо себя незараженные участки
Вирусы-призраки	Не имеют ни одного постоянного участка кода, труднообнаруживаемы, основное тело вируса зашифровано
Макровирусы	Пишутся не в машинных кодах, а на WordBasik, живут в документах Word, переписывают себя в Normal.dot

Основными путями проникновения вирусов в компьютер являются съемные диски (гибкие и лазерные), а также компьютерные сети. При заражении компьютера вирусом важно его обнаружить по характерным признакам.

Признаками воздействия вирусов на компьютерную систему служат следующие:

- изменение даты создания и длины файла;
- пропажа файла;
- слишком частые обращения к диску;
- непонятные ошибки;
- «зависание» компьютера;
- самопроизвольная перезагрузка операционной системы;
- замедление работы процессора;
- появление неожиданных графических и звуковых эффектов;
- сообщения антивирусных программ;

- сообщение, требующее выплаты компенсации за восстановление файлов компьютеров (вирусы-вымогатели).

Все действия вируса могут выполняться достаточно быстро и без выдачи каких-либо сообщений, поэтому пользователю очень трудно заметить, что в компьютере происходит что-то необычное.

Пока на компьютере заражено относительно мало программ, наличие вируса может быть практически незаметно. Однако по прошествии некоторого времени на компьютере начинает твориться что-то странное, например:

- некоторые программы перестают работать или начинают работать неправильно;
- на экран выводятся посторонние сообщения, символы и т.д.;
- работа на компьютере существенно замедляется и может быть прекращена (вирусы-вымогатели);
- некоторые файлы оказываются испорченными и т.д.

К этому моменту, как правило, уже достаточно много (или даже большинство) программ являются зараженными вирусом, а некоторые файлы и диски – испорченными. Более того, зараженные программы с одного компьютера могли быть перенесены с помощью дискет или по сети на другие компьютеры.

Некоторые виды вирусов ведут себя еще более коварно. Они вначале незаметно заражают большое число программ или дисков, а потом причиняют очень серьезные повреждения, например, формируют весь жесткий диск на компьютере. А бывают вирусы, которые стараются вести себя как можно более незаметно, но понемногу и постепенно портят данные на жестком диске компьютера.

Большинство вирусов не выполняет каких-либо действий, кроме своего распространения (заражения других программ, дисков и т.д.) и. иногда, выдачи каких-либо сообщений или иных эффектов, придуманных автором вируса: игры, музыки, перезагрузки компьютера, выдачи на экран разных рисунков, блокировки или изменения функций клавиш клавиатуры, замедления работы компьютера и т.д. Однако сознательной порчи информации эти вирусы не осуществляют. Такие вирусы условно называются ***неопасными***. Впрочем, и эти вирусы способны причинить большие неприятности (например, перезагрузки каждые несколько минут вообще не дадут вам работать).

Однако около трети всех видов вирусов портят данные на дисках – или сознательно, или из-за содержащихся в вирусах ошибок, скажем, из-за не вполне корректного выполнения некоторых действий. Если порча данных происходит лишь эпизодически и не приводит к тяжелым последствиям, то вирусы называются ***опасными***. Если же порча данных происходит часто или вирусы причиняют значительные разрушения (форматирование жесткого диска, систематическое изменение данных на диске и т.д.), то вирусы называются ***очень опасными***.

История компьютерной вирусологии представляется сегодня постоянной «гонкой за лидером», причем, не смотря на всю мощь современных антивирусных программ, лидерами являются именно вирусы. Среди тысяч вирусов лишь несколько десятков являются оригинальными разработками, использующими действительно принципиально новые идеи. Все остальные - «вариации на тему». Но каждая оригинальная разработка заставляет создателей антивирусов приспосабливаться к новым условиям, догонять вирусную технологию.

Как и предсказывалось, все большие обороты набирает развитие червей и троянцев для мобильных телефонов. В настоящий момент количество вредоносных программ увеличивается примерно на 1 новую программу в неделю.

Примечателен тот факт, что в антивирусные базы были добавлены представители нового класса червей для мобильных телефонов под управлением операционной системы Symbian. Речь идет о «почтовых мобильных червях», использующих для самораспространения MMS (сервис передачи мультимедийных сообщений). В обнаруженные экземпляры встроено два способа распространения. Первый, уже ставший традиционным для мобильных червей, через протокол Bluetooth; червь распространяется, рассылая себя на все доступные устройства в радиусе 10-15 метров. Второй – при помощи MMS – сообщений.

В настоящий момент известно два семейства MMS-червей:

- Comwar, который рассылает себя по всей адресной книге мобильного телефона;
- Cabir.k, который ведет себя более оригинально, а именно – ждет прихода на телефон SMS- или MMS-сообщения и отправляет себя в ответ на него.

Начавшись с одного единственного Bluetooth-червя, вредоносные программы для мобильных устройств сейчас представлены сразу 3-мя классами: Worm (причем, здесь теперь есть как «сетевые» черви, так и «почтовые»), Virus, Trojan.

Если традиционным вирусам потребовались годы, чтобы прийти к такому количеству поведений, то мобильные вирусы проделали этот путь менее чем за год.

Можно с уверенностью прогнозировать, что в ближайший год появятся мобильные представители других классов компьютерных вирусов.

Справочник угроз при работе в интернет

В прошлом компьютерам угрожали преимущественно вирусы и черви. Основной целью этих программ было самораспространение; некоторые программы также причиняли вред файлам и самим компьютерам. Такие вредоносные программы – типичные проявления кибервандализма.

В чем разница между вирусом и червем?

Вирус – это саморазмножающаяся программа, она распространяется с файла на файл и с компьютера на компьютер. Кроме того, вирус может быть запрограммирован на уничтожение или повреждение данных.

Черви считаются подклассом вирусов, но обладают характерными особенностями. Червь размножается (воспроизводит себя), не заражая другие файлы. Он внедряется один раз на конкретный компьютер и ищет способы распространиться далее на другие компьютеры.

Вирус заражает тем большее количество файлов, чем дольше он находится на компьютере необнаруженным. Червь создает единственную копию своего кода. В отличие от вируса, код червя самостоятелен. Другими словами, червь – это отдельный файл, в то время как вирус – это код, который внедряется в существующие файлы.

Что такое рекламные системы (adware)?

Понятие «adware» включает в себя программы, запускающие рекламу (часто в виде всплывающих окон) или перенаправляющие поисковые запросы на рекламные веб-сайты. Рекламное ПО часто бывает встроено в бесплатные или условно-бесплатные программы и устанавливается на компьютер пользователя одновременно с основным приложением без

ведома и согласия пользователя. В некоторых случаях рекламное ПО может тайно загрузить и установить на ваш компьютер троянская программа.
Устаревшие, не обновленные вовремя версии веб-браузеров могут быть уязвимыми для хакерских инструментов, скачивающих рекламные программы на ваш компьютер.

Контрольные вопросы к теме 2

1. Назовите информационные угрозы для государства.
2. Какие создаются информационные угрозы для компании?
3. Что угрожает личности (физическому лицу)?
4. Назовите причины информационных угроз.
5. Какие действия и события нарушают ИБ?
6. Какие личностно-профессиональные характеристики сотрудников способствуют реализации угроз ИБ?
7. Назовите основные компьютерные вирусы.
8. Какие вы знаете компьютерные преступления?

Тесты к теме 2

1.Несанкционированным доступом является:

А. недостаточное знание работниками предприятия правил защиты информации;
Б. слабый контроль за соблюдением правил защиты информации;
В. хищение носителей информации и документальных отходов.

2. Реализации угроз информационной безопасности способствуют:
А. болтливость;
Б. простудные заболевания;
В. Налоговый кодекс.

3. Типовыми путями несанкционированного доступа к информации, являются:
А. дистанционное фотографирование;
Б. выход из строя ПЭВМ;
В. ураганы.

4. Несанкционированным доступом к информации НЕ является:
А. использование программных ловушек;
Б. любительское фотографирование;
В. включение в библиотеки программ специальных блоков типа «троянский конь».

5. К способам воздействия угроз на информационные объекты НЕ относятся:
А. программно-математические;
Б. организационно-правовые;
В. договорные отношения.

6. Хакерная война – это?

А. атака компьютеров и сетей гражданского информационного пространства;
Б. использование информации для влияния на умы союзников и противников;
Б. блокирование информации, преследующее цель получить экономическое превосходство.

7. Угрозы доступности данных возникают в том случае, когда?
А. объект не получает доступа к законно выделенным ему ресурсам;
Б. легальный пользователь передает или принимает платежные документы, а потом отрицает это, чтобы снять с себя ответственность;
В. случаются стихийные бедствия.

8. Внедрение компьютерных вирусов является следующим способом воздействия угроз на информационные объекты?
А. информационным;
Б. физическим;
В. программно-математическим способом.

9. Логическая бомба – это?
+А. компьютерный вирус;
Б. способ ведения информационной войны;
В. прием, используемый в споре на философскую тему.

10. Объектом информационной атаки не является:
А. АИС в целом;
Б. каналы передачи данных;
В. природоохранные мероприятия.

11. Под «маскарадом» понимается?
А. выполнение каких-либо действий одним пользователем от имени другого пользователя;
Б. обработка денежных счетов при получении дробных сумм;
В. монополизация какого-либо ресурса системы.

12. «Люком» называется?
А. использование после окончания работы части данных, оставшиеся в памяти;
Б. передача сообщений в сети от имени другого пользователя;
В. не описанная в документации на программный продукт возможность работы с ним.

13. «Мобильные» вирусы распространяются:
А. путем взлома программ ВЭВМ;
Б. в виде «червей» и «троянцев» для мобильных телефонов;
В. по линии связи между узлами сети.

14.Для компьютерных преступлений НЕ характерна:
А. сложность сбора доказательств;
Б. наличие достаточной следственной практики по раскрытию компьютерных преступлений в РФ;

В. высокая латентность.