# 5. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

## 5.1. Классификация угроз информационной безопасности

Угрозы информационной (компьютерной) безопасности — это различные действия, которые могут привести к нарушениям состояния защиты информации. Другими словами, это — потенциально возможные события, процессы или действия, которые могут нанести ущерб информационным и компьютерным системам.

Угрозы ИБ можно разделить на два типа: естественные и искусственные. К естественным относятся природные явления, которые не зависят от человека, например, ураганы, наводнения, пожары и т.д. Искусственные угрозы зависят непосредственно от человека и могут быть преднамеренными и непреднамеренными. Непреднамеренные угрозы возникают из-за неосторожности, невнимательности и незнания. Примером таких угроз может быть установка программ, не входящих в число необходимых для работы и в дальнейшем нарушающих работу системы, что и приводит к потере информации. Преднамеренные угрозы, в отличие от предыдущих, создаются специально. К ним можно отнести атаки злоумышленников как извне, так и изнутри компании. Результат реализации этого вида угроз — потери денежных средств и интеллектуальной собственности организации.

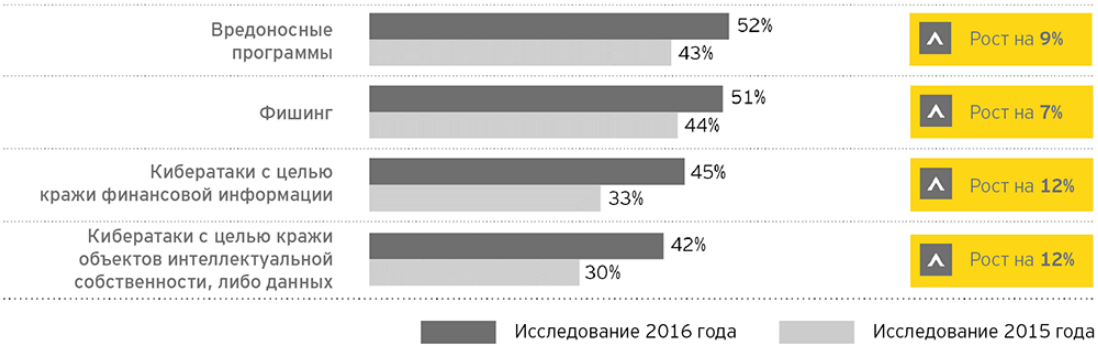
**Классификация угроз информационной безопасности**

В зависимости от различных способов классификации все возможные угрозы информационной безопасности можно разделить на следующие основные подгруппы.

- Нежелательный контент.
- Несанкционированный доступ.
- Утечки информации.
- Потеря данных.
- Мошенничество.

- Кибервойны.
- Кибертерроризм.

Нежелательный контент — это не только вредоносный код, потенциально опасные программы и спам (т.е. то, что непосредственно создано для уничтожения или кражи информации), но и сайты, запрещенные законодательством, а также нежелательные ресурсы с информацией, не соответствующей возрасту потребителя.




Несанкционированный доступ — просмотр информации сотрудником, который не имеет разрешения пользоваться ею, путем превышения должностных полномочий. Несанкционированный доступ приводит к утечке информации. В зависимости от того, каковы данные и где они хранятся, утечки могут организовываться разными способами, а именно через атаки на сайты, взлом программ, перехват данных по сети, использование несанкционированных программ.


Утечки информации можно разделять на умышленные и случайные. Случайные утечки происходят из-за ошибок оборудования, программного обеспечения и персонала. Умышленные, в свою очередь, организовываются преднамеренно с целью получить доступ к данным, нанести ущерб.

Потерю данных можно считать одной из основных угроз информационной безопасности. Нарушение целостности информации может быть вызвано неисправностью оборудования или умышленными действиями людей, будь то сотрудники или злоумышленники.

Не менее опасной угрозой является мошенничество с использованием информационных технологий ("фрод"). К мошенничеству можно отнести не только манипуляции с кредитными картами ("кардинг") и взлом онлайн-банка, но и внутренний фрод. Целями этих экономических преступлений являются обход законодательства, политики безопасности или нормативных актов, присвоение имущества.

Ежегодно по всему миру возрастает террористическая угроза, постепенно перемещаясь при этом в виртуальное пространство. На сегодняшний день никого не удивляет возможность атак на автоматизированные системы управления технологическими процессами

(АСУ ТП) различных предприятий. Но подобные атаки не проводятся без предварительной разведки, для чего применяется кибершпионаж, помогающий собрать необходимые данные. Существует также такое понятие, как "информационная война"; она отличается от обычной войны тем, что в качестве оружия выступает тщательно подготовленная информация.

## 5.2. Компьютерные вирусы и защита от них

**Компьютерные вирусы** – специально написанные программы, способные самопроизвольно присоединяться к другим программам, создавать свои копии и внедрять их в файлы, системные области компьютера и в вычислительные сети с целью нарушения работы программ, порчи файлов и каталогов, создания всевозможных помех в работе компьютера. Могут быть разрушительными или проявляться в виде помехи, например,

- замена и/или удаление части или всего файла;
- форматирование диска;
- разрушение таблицы размещения файлов FAT);
- искажение сообщений программы пользователя и т. п.

Вирусы-помехи могут выводить на экран информацию, затрудняющую чтение сообщений программ. В настоящее время насчитывается несколько тысяч различных вирусов, и их количество продолжает возрастать. Например, только в глобальной сети Internet ежемесячно появляются не менее 200 вирусов.

**Способы распространения компьютерных вирусов**

Возможные каналы проникновения вирусов в компьютер – накопители на сменных носителях информации, главным образом на дискетах, а также средства межкомпьютерной связи.

К последним относятся компьютерные сети, электронная почта, система BBS (Bulletin Board System – доска объявлений) и любая другая непосредственная связь между компьютерами.

Наиболее опасным является распространение вирусов по компьютерной сети, так как в этом случае за короткий промежуток времени может быть заражено большое количество компьютеров. Имеются даже специальные сетевые вирусы, предназначенные для функционирования в сетях.

При запуске инфицированной программы вирус старается отыскать незараженные программы и внедриться в них, а затем производит разрушительные действия.

**Классификация компьютерных вирусов**

**Компьютерный вирус** – это программный код, встроенный в другую программу, в документ, или в определенные области носителя данных и предназначенный для выполнения несанкционированных действий на несущем компьютере.

Так, например, вирусный код может воспроизводить себя в теле других программ (этот процесс называется *размножением*). По прошествии определенного времени, создав достаточное количество копий, программный вирус может перейти к разрушительным действиям – нарушению работы программ и операционной системы, удалению информации, хранящейся на жестком диске и т.д. Этот процесс называется *вирусной атакой*.

Вирусы классифицируют по различным признакам.

**1. По среде обитания**

- ***Сетевые*** вирусы распространяются по различным сетям, т.е. при передаче информации с одного компьютера на другой, соединенные между собой сетью, например, Интернет.
- ***Файловые*** вирусы заражают исполнительные файлы и загружаются после запуска той программы, в которой он находится. Файловые вирусы могут внедряться и в другие файлы, но записанные в таких файлах, они не получают управление и теряют способность к размножению.

- ***Загрузочные*** вирусы внедряются в загрузочный сектор дискет или логических дисков, содержащий программу загрузки.
- ***Файлово – загрузочные*** вирусы заражают одновременно файлы и загрузочные сектора диска.

**2. По способу заражения среды обитания.**

- ***Резидентный вирус*** при заражении компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т.п.) и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера.
- ***Нерезидентный вирус*** не заражает память компьютера и является активным ограниченное время. Активизируется в определенные моменты, например, при обработке документов текстовым редактором.

**3. По деструктивным (разрушительным) возможностям**

- ***Безвредные*** вирусы проявляются только в том, что уменьшают объем памяти на диске в результате своего распространения.
- ***Неопасные***, так же уменьшают объем памяти, не мешают работе компьютера, такие вирусы порождают графические, звуковые и другие эффекты.
- ***Опасные вирусы***, которые могут привести к различным нарушениям в работе компьютера, например, к зависанию или неправильной печати документа.
- ***Очень опасные***, действие которых может привести к потере программ, данных, стиранию информации в системных областях памяти и даже приводить к выходу из строя движущихся частей жесткого диска при вводе в резонанс.

**4. По особенностям алгоритма**

- **Паразитические** – это одни из самых простых вирусов. Они изменяют содержимое файлов и секторов диска и могут быть достаточно легко

обнаружены и уничтожены.

- **Вирусы-репликаторы** (черви) распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии.
- **Вирусы невидимки** (стелс-вирусы) – вирусы, которые очень трудно обнаружить и обезвредить, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего незараженные участки диска.
- **Мутанты** (призраки) содержат алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов. Такие вирусы самые сложные в обнаружении.
- **Троянские программы** (квазивирусы) не способны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков.
- **Спутники** – вирус, который не изменяет файл, а для выполнимых программ (exe) создают одноименные программы типа com, которые при выполнении исходной программы запускаются первыми, а затем передают управление исходной выполняемой программе.
- **Студенческие вирусы** представляют собой самые простые и легко обнаруживаемые вирусы.

Однако четкого разделения между ними не существует, и все они могут составлять комбинацию вариантов взаимодействия – своеобразный вирусный "коктейль".

**5. 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 Microsoft Word. Заражение происходит при открытии файла

документа в окне программы, если в ней не отключена возможность исполнения макрокоманд. Как и для других типов вирусов, результат атаки может быть, как относительно безобидным, так и разрушительным.

**Защита от компьютерных вирусов**

Компьютерный вирус аналогичен природному вирусу. Поэтому меры защиты от него включают в себя аналогичный комплекс средств:

- Профилактика;
- Диагностика;
- Лечение.

**Профилактика**

К профилактическим средствам относятся:

- перекрытие путей проникновения вирусов в компьютер;
- исключение возможности заражения и порчи вирусами, проникшими в компьютер, других файлов.

**Диагностика**

Диагностические средства позволяют обнаруживать вирусы в компьютере и распознавать их тип.

**Лечение**

Лечение состоит в удалении вирусов из зараженных программных средств и восстановлении пораженных файлов.

Защитный комплекс основывается на применении антивирусных программ и проведении организационных мероприятий.

**Организационные мероприятия, производимые для защиты от компьютерных вирусов**

Вирусы попадают в компьютер только вместе с программным обеспечением. Поэтому самым важным в защите от вирусов является *использование незараженных программ,* так как главным источником вирусов являются незаконные, так называемые "пиратские" копии программного обеспечения.

Особенно опасны компьютерные игры и различного рода

развлекательные программы, которые чаще других являются разносчиками компьютерной инфекции. Поэтому первым и наиважнейшим правилом антивирусной защиты является следующее:

***Необходимо использовать только лицензионно-чистые программы от надежных поставщиков.***

**Рекомендации**

- приобретайте все программы в фирменной упаковке у надежного поставщика;
- не пользуйтесь без крайней необходимостью чужими дискетами;
- не запускайте на выполнение программы, назначение которых неизвестно или непонятно;
- не передавайте свои дискеты чужим лицам для использования, чтобы не заразить ваши дискеты;
- ограничьте доступ к вашему ПК посторонних лиц и запретите им пользоваться своими дискетами без вашего разрешения;
- перед началом работы на ПК после другого лица осуществите холодный перезапуск ПК, чтобы удалить из ОЗУ возможно присутствующие там резидентные вирусы;
- при работе на одном ПК нескольких пользователей, разделите жесткий диск на несколько логических и разграничьте право доступа к различным дискам;
- включайте программы антивирусной защиты в файл AUTOEXEC. BAT;
- не ограничивайтесь использованием только одного антивирусного программного продукта. Новые вирусы появляются постоянно, и для их выявления требуются новые антивирусные программы;
- гибкие магнитные диски используйте, по возможности, с защитой от записи.

## 5.3. Вирусоподобные программы

К "вредным программам", помимо вирусов, относятся:

- "троянские программы" (логические бомбы);
- утилиты скрытого администрирования удаленных компьютеров;
- "intended"-вирусы;
- конструкторы вирусов;
- полиморфик-генераторы.

**"Троянские" программы (логические бомбы).** К "троянским" программам относятся программы, наносящие какие-либо разрушительные действия в зависимости от каких-либо условий. Например, уничтожение информации на дисках при каждом запуске или по определенному графику и т. д. Большинство известных "троянских" программ являются программами, которые маскируются под какие-либо полезные программы, новые версии популярных утилит или дополнения к ним. Очень часто они рассылаются по электронным конференциям. По сравнению с вирусами "троянские" программы не получают широкого распространения по достаточно простым причинам – они либо уничтожают себя вместе с остальными данными на диске, либо демаскируют свое присутствие и уничтожаются пострадавшим пользователем. К "троянским" программам также относятся так называемые "дропперы" вирусов – зараженные файлы, код которых подправлен таким образом, что известные версии антивирусов не определяют присутствие вируса в файле. Например, файл шифруется или упаковывается неизвестным архиватором, что не позволяет антивирусу "увидеть" заражение.

Отметим еще один тип программ (программы – "злые шутки"), которые используются для устрашения пользователя, свидетельствуя о заражении вирусом или о каких-либо предстоящих действиях с этим связанных, то есть сообщают о несуществующих опасностях, вынуждая пользователя к активным действиям. Например, к "злым шуткам" относятся программы, которые "пугают" пользователя сообщениями о форматировании диска (хотя никакого форматирования на самом деле не происходит), детектируют вирусы в

незараженных файлах, выводят странные вирусоподобные сообщения и т. д. К категории "злых шуток" можно отнести также заведомо ложные сообщения о новых "супер-вирусах". Такие сообщения периодически появляются в сети Интернет и обычно вызывают панику среди пользователей.

**Утилиты скрытого администрирования.** Утилиты скрытого администрирования являются разновидностью "логических бомб" ("троянских программ"), которые используются злоумышленниками для удаленного администрирования компьютеров в сети. По своей функциональности они во многом напоминают различные системы администрирования, разрабатываемые и распространяемые различными фирмами-производителями программных продуктов. Единственная особенность этих программ заставляет классифицировать их как вредные "троянские" программы: отсутствие предупреждения об инсталляции и запуске. При запуске такая программа устанавливает себя в систему и затем следит за ней, при этом пользователю не выдается никаких сообщений о действиях программы в системе. Чаще всего ссылка на такую программу отсутствует в списке активных приложений. В результате пользователь может и не знать о ее присутствии в системе, в то время как его компьютер открыт для удаленного управления.

Внедренные в операционную систему утилиты скрытого управления позволяют делать с компьютером все что в них заложил их автор: принимать/отсылать файлы, запускать и уничтожать их, выводить сообщения, стирать информацию, перезагружать компьютер и т.д. в результате эти программы могут быть использованы для обнаружения и передачи конфиденциальной информации, для запуска вирусов, уничтожения данных и т.п.

**"Intended"-вирусы**. К таким вирусам относятся программы, которые, на первый взгляд, являются стопроцентными вирусами, но не способны размножаться по причине ошибок. Например, вирус, который при заражении не помещает в начало файла команду передачи управления на код вируса, либо

записывает в нее неверный адрес своего кода, либо неправильно устанавливает адрес перехватываемого прерывания (в большинстве приводит к "зависанию" компьютера) и т. д. К категории "intended" также относятся вирусы, которые по приведенным выше причинам размножаются только один раз – из "авторской" копии. Заразив какой-либо файл, они теряют способность к дальнейшему размножению. Появляются "intended"-вирусы чаще всего из-за неумелой перекомпиляции какого-либо уже существующего вируса, либо по причине недостаточного знания языка программирования, либо по причине незнания технических тонкостей операционной системы.

**Конструкторы вирусов**. К данному виду "вредных" программ относятся утилиты, предназначенные для изготовления новых компьютерных вирусов. Известны конструкторы вирусов для DOS, Windows и макровирусов. Они позволяют генерировать исходные тексты вирусов, объектные модули, и/или непосредственно зараженные файлы. Некоторые конструкторы снабжены стандартным оконным интерфейсом, где при помощи системы меню можно выбрать тип вируса, поражаемые объекты (COM и/или EXE), наличие или отсутствие самошифровки, противодействие отладчику, внутренние текстовые строки, выбрать эффекты, сопровождающие работу вируса, и т. п.

**Полиморфные генераторы**. Полиморфик-генераторы, как и конструкторы вирусов, не являются вирусами в прямом смысле этого слова, поскольку в их алгоритм не закладываются функции размножения, т. е. открытия, закрытия и записи в файлы, чтения и записи секторов и т. д. Главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика. Обычно полиморфные генераторы распространяются в виде файла-архива. Основным файлом в архиве любого генератора является объектный модуль, содержащий этот генератор.