Содержание:

Введение

Сегодня категория «информация» нередко определяется как нечто, дающее нам представление об окружающем мире и его составляющих. К таким составляющим относятся различные явления и предметы, другие люди, представители флоры и фауны и вообще все, что мы можем ощутить при помощи органов чувств.

Не так давно информация перешла в новый для человечества формат – в электронный формат. И это стало одновременно и спасением, и проклятием. Так, с одной стороны, человечество сделало несравненно значительный шаг вперед, получив возможность обрабатывать информацию в миллионы раз быстрее, чем раньше – мы можем узнать практически все за считанные секунды, можем общаться с людьми, находящимися на другом конце света. Новые информационные технологии перевернули также представление о медицине, науке и технике, и вообще во многих сферах жизни общества сегодня мы можем делать то, о чем раньше и не мечтали. С другой же стороны, мы получили еще одну уязвимую сторону жизни. Информация, хранящаяся в электронном виде, подвержена значительному числу угроз. Частная жизнь может стать достоянием общественности, корпоративная и даже государственная тайна могут быть раскрыты в считанные минуты, что приведет к непредсказуемым последствиям.

Одним из наиболее угрожающих факторов сложившейся ситуации является то, что угроз информации, ее целостности и достоверности великое множество, и не все они носят преднамеренный характер. В связи с этим изучение видов и состава угроз информационной безопасности является сегодня более чем актуальной темой для исследования.

Таким образом, цель работы – рассмотрение видов и состава угроз информационной безопасности. Для достижения данной цели выполним следующие задачи:

- рассмотреть понятие и сущность информации;
- проанализировать суть информационной безопасности;
- охарактеризовать понятие угрозы информационной безопасности;
- рассмотреть классификацию и состав угроз информационной безопасности;

- подвести итоги по выполненной работе.

Структура работы включает себя две главы, каждая из которых, в свою очередь, состоит из двух параграфов. Кроме того, в структуру работы включаются такие элементы, как Введение, Заключение и Список использованной литературы. Общий объем работы составляет 25 страниц.

Методологической основой работы являются предложенные методические рекомендации. Теоретическая основа – теоретические научные труды известных исследователей таких проблем как информация, информационная безопасность, защита информации и т.д.

Понятие и сущность информационной безопасности

- 1.

Понятие и сущность информации

Категория «информация» является базовой во всех информационных технологиях. Так или иначе, любой вид деятельности и познания человека является процессом сбора и обработки информации, после чего становится возможным адекватное ситуации поведение, принятие решений и их реализация. Современные информационные средства сделали информацию, помимо всего прочего, одним из наиболее значимых и ценных ресурсов в научно-техническом, коммерческом, политическом и др. мире.

Обмен данными характерен всем живым существам, и, в особенности – человечеству. Для человека информация, полученная из различных источников, сама становится источником новых знаний. С философской точки зрения информация сегодня стала одной из исходных категорий мироздания и теперь стоит в одном ряду с такими категориями, как «материя» и «энергия». При этом все три названные сущности переплетаются, образуя тесную связь, которые можно увидеть и в природных, и в антропогенных творениях. Так или иначе, все человеческие действия и поступки – от ежедневных бытовых ритуалов до запуска ракет в космос – влияют на увеличение информации в мире, и объем этой информации растет значительно более стремительно, чем население Земли или

даже материальные потребности человечества.

До начала промышленной революции, определение сути информации оставалось прерогативой преимущественно философов [5]. Затем, понятие информации стало активно использоваться в технических и гуманитарных науках. В середине XX века рассматривать вопросы теории информации стали новые на то время науки: теория передачи информации и кибернетика.

Особенностью понятия «информация» является его универсальность – оно используется во всех без исключения сферах человеческой деятельности: в философии, естественных и гуманитарных науках, в биологии, медицине, в психологии человека и животных, в социологии, искусстве, в технике и экономике и, конечно, в повседневной жизни.

В настоящее время среди людей не существует единого определения термина информация, так как каждый понимает ее чисто интуитивно, не имея представления о ее научном определении. С точки зрения различных прикладных областей деятельности, данное понятие описывается своим специфическим набором признаков, конкретизированных для частного применения.

В информатике широко используется такое определение: «информация – сведения, передаваемые источником получателю (приёмнику)» [7]. Информация всегда связана с материальным носителем, с материальными процессами и имеет некоторое представление (форму). Информация, представленная в какой–либо законченной (системной) форме и передаваемая из одного места в другое, называется сообщением. Сообщения представляются в виде сигналов и данных. Сигналы используются для передачи информации в пространстве между источником и получателем, а данные – для хранения (то есть для передачи во времени).

Качество информации является одним из важнейших параметров для потребителя информации. Оно определяется следующими характеристиками:

- репрезентативность – правильность отбора информации в целях адекватного отражения источника информации;
- содержательность – семантическая емкость информации. Рассчитывается как отношение количества семантической информации к ее количеству в статистической мере;
- достаточность (полнота) – минимальный, но достаточный состав данных для достижения целей, которые преследует потребитель информации;

- доступность – простота (или возможность) выполнения процедур получения и преобразования информации;
- актуальность – зависит от динамики изменения характеристик информации и определяется сохранением ценности информации для пользователя в момент ее использования;
- своевременность – поступление не позже заранее назначенного срока;
- точность – степень близости информации к реальному состоянию источника информации;
- достоверность – свойство информации отражать источник информации с необходимой точностью;
- устойчивость – способность информации реагировать на изменения исходных данных без нарушения необходимой точности.
- прагматичность – выгодность информации, ее полезность [7].
    1.

Суть информационной безопасности

В повседневной жизни часто информационная безопасность (далее – ИБ) понимается лишь как необходимость борьбы с утечкой секретной и распространением ложной и враждебной информации. Однако, это понимание очень узкое. Существует много разных определений информационной безопасности, в которых высвечиваются отдельные её свойства.

Согласно ГОСТ Р 50922-96 «Защита информации. Основные термины и определения» под информационной безопасностью понималось состояние защищённости информационной среды общества, обеспечивающее её формирование и развитие в интересах граждан, организаций и государства [1].

Информационная безопасность – защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб владельцам или пользователям информации и поддерживающей инфраструктуры.

Меры по обеспечению информационной безопасности должны осуществляться в разных сферах – политике, экономике, обороне, а также на различных уровнях – государственном, региональном, организационном и личностном. Поэтому задачи информационной безопасности на уровне государства отличаются от задач, стоящих перед информационной безопасностью на уровне организации.

Субъект информационных отношений может пострадать (понести материальные и/или моральные убытки) не только от несанкционированного доступа к информации, но и от поломки системы, вызвавшей перерыв в работе. ИБ зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электро–, водо– и теплоснабжения, кондиционеры, средства коммуникаций и, конечно, обслуживающий персонал. Поддерживающая инфраструктура имеет самостоятельную ценность, важность которой переоценить невозможно [12].

После событий 11 сентября 2001 года в законодательстве США в соответствии с законом «О патриотизме» было определено понятие «критическая инфраструктура», которая понимается как «совокупность физических или виртуальных систем и средств, важных для США в такой мере, что их выход из строя или уничтожение могут привести к губительным последствиям в области обороны, экономики, здравоохранения и безопасности нации» [12]. Понятие критической инфраструктуры охватывает такие ключевые области народного хозяйства и экономики США, как национальная оборона, сельское хозяйство, производство пищевых продуктов, гражданская авиация, морской транспорт, автомобильные дороги и мосты, тоннели, дамбы, трубопроводы, водоснабжение, здравоохранение, службы экстренной помощи, органы государственного управления, военное производство, информационные и телекоммуникационные системы и сети, энергетика, транспорт, банковская и финансовая системы, химическая промышленность, почтовая служба [12].

В социальном плане информационная безопасность предполагает борьбу с информационным «загрязнением» окружающей среды, использованием информации в противоправных и аморальных целях.

Объектом ИБ будет считаться информация, затрагивающая государственные, служебные, коммерческие, интеллектуальные и личностные интересы, а также средства и инфраструктура её обработки и передачи. Также объектами информационного воздействия и, следовательно, информационной безопасности могут быть общественное или индивидуальное сознание.

Общественное сознание – совокупность идей, взглядов, представлений, существующих в обществе в данный период, в которых отражается социальная действительность [5].

На государственном уровне субъектами ИБ являются органы исполнительной, законодательной и судебной власти. В отдельных ведомствах созданы органы, специально занимающиеся информационной безопасностью.

Кроме этого, субъектами ИБ могут быть:

- граждане и общественные объединения;
- средства массовой информации;
- предприятия и организации независимо от формы собственности.

Интересы субъектов ИБ, связанных с использованием информационных систем, можно подразделить на следующие основные категории:

1. Доступность – возможность за приемлемое время получить требуемую информационную услугу. Информационные системы создаются (приобретаются) для получения определенных информационных услуг (сервисов). Если по тем или иным причинам получение этих услуг пользователями становится невозможным, это наносит ущерб всем субъектам информационных отношений. Особенно ярко ведущая роль доступности проявляется в разного рода системах управления: производством, транспортом и т.п. Поэтому, не противопоставляя доступность остальным аспектам, доступность является важнейшим элементом ИБ.
2. Целостность –актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения. Целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий (транзакций)). Практически все нормативные документы и отечественные разработки относятся к статической целостности, хотя динамический аспект не менее важен. Пример области применения средств контроля динамической целостности – анализ потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений.
3. Конфиденциальность – защита от несанкционированного ознакомления. На страже конфиденциальности стоят законы, нормативные акты, многолетний опыт соответствующих служб. Аппаратно–программные продукты позволяют закрыть практически все потенциальные каналы утечки информации [9].

Цель мероприятий в области информационной безопасности – защита интересов субъектов ИБ.

Задачи ИБ:

1. Обеспечение права личности и общества на получение информации.
2. Обеспечение объективной информацией.
3. Борьба с криминальными угрозами в сфере информационных и телекоммуникационных систем, с телефонным терроризмом, отмыванием денег и т.д.
4. Защита личности, организации, общества и государства от информационно–психологических угроз.
5. Формирование имиджа, борьба с клеветой, слухами, дезинформацией [9].

В первой главе работы определено, что информация является базовым понятием во всем мире информационных технологий – как в практической реализации, так и в научной сфере. Так, информация в информационных технологиях представляет собой сведения, которые передаются от источника приемнику. Информация в данном случае может передаваться от пользователя компьютеру и наоборот, данные также курсируют между аппаратными средствами функционирования компьютера и по многим другим каналам. И каждый из этих каналов должен быть достаточно надежным и защищенным, чтобы можно было говорить о реализации информационной безопасности – состояния, в котором информация и вся поддерживающая ее инфраструктура находится в защищенном состоянии, как от случайного, так и преднамеренного вредоносного влияния. Целостное понятие информации и состояния ее безопасности позволяют продолжить исследование более объективно и рассмотреть, что именно представляют собой угрозы безопасности, какого они бывают вида и состава.

Угрозы информационной безопасности

2.1 Угрозы информационной безопасности. Понятие

Угроза информационной безопасности представляет собой совокупность действий, которые могут привести к нарушению информационной безопасности [2]. Иначе говоря, угроза информационной безопасности является совокупностью потенциально возможных событий, процессов или действий, которая может нанести ущерб информации, информационным и компьютерным системам.

Первоначально угрозы информационной безопасности делятся на естественные и искусственные. Естественные угрозы информационной безопасности это, в первую очередь, явления природы, не зависящие от человека. Сюда можно отнести цунами, землетрясения, пожары и т.д. Искусственные угрозы являются своего рода противоположностью естественных угроз – они вызваны намеренными или непреднамеренными действиями человека. Непреднамеренные угрозы информационной безопасности могут реализовываться как следствие невнимательности, некомпетентности, иначе говоря – как следствие влияния человеческого фактора. Преднамеренные же угрозы, как следует из самого названия, реализуются с определенным намерением, и, естественно, в подавляющем числе случаев, намерение это вредительского характера. Такими угрозами могут быть атаки злоумышленников, промышленный шпионаж, кибертерроризм и др. [2].

Нарушение информационной безопасности может быть вызвано как спланированными действиями злоумышленника, так и неопытностью сотрудника. Пользователь должен иметь хоть какое–то понятие об ИБ, вредоносном программном обеспечении, чтобы своими действиями не нанести ущерб компании и самому себе. Чтобы пробиться через защиту и получить доступ к нужной информации злоумышленники используют слабые места и ошибки в работе программного обеспечения, веб–приложений, ошибки в конфигурациях файрволов, прав доступа, прибегают к прослушиванию каналов связи и использованию клавиатурных шпионов.

Потеря информации может быть обусловлена не только внешними атаками злоумышленников и неаккуратностью сотрудников, но и работниками компании, которые заинтересованы в получении прибыли в обмен на ценные данные организации, в которой работают или работали. Источниками угроз выступают киберпреступные группы и государственные спецслужбы (киберподразделения), которые используют весь арсенал доступных киберсредств: нежелательный контент; несанкционированный доступ; утечки информации; потеря данных; мошенничество; кибервойны и кибертерроризм [16].

То, чем будет производиться атака, зависит от типа информации, ее расположения, способов доступа к ней и уровня защиты. Если атака будет рассчитана на неопытность жертвы, то возможно использование спам рассылок. Оценивать угрозы информационной безопасности необходимо комплексно, при этом методы оценки будут различаться в каждом конкретном случае. Например, чтобы исключить потерю данных из–за неисправности оборудования, нужно использовать

качественные комплектующие, проводить регулярное техническое обслуживание, устанавливать стабилизаторы напряжения.

Дальше следует устанавливать и регулярно обновлять программное обеспечение. Отдельное внимание нужно уделить защитному ПО, базы которого должны обновляться ежедневно: защита от нежелательного контента (антивирус, антиспам, веб–фильтры, анти–шпионы) фаерволы и системы обнаружения вторжений IPS IDM PUM защита веб–приложений анти–ддос WAF анализ исходного кода антифрод защита от таргетированных атак SIEM системы обнаружения аномального поведения пользователей (UEBA) защита АСУ ТП защита от утечек данных DLP шифрование защита мобильных устройств резервное копирование системы отказоустойчивости Обучение сотрудников компании основным понятиям информационной безопасности и принципам работы различных вредоносных программ поможет избежать случайных утечек данных, исключить случайную установку потенциально опасных программ на компьютер. Также в качестве меры предосторожности от потери информации следует делать резервные копии. Для того чтобы следить за деятельностью сотрудников на рабочих местах и иметь возможность обнаружить злоумышленника, следует использовать DLP–системы [16].

Организовать информационную безопасность помогут специализированные программы, разработанные на основе современных технологий. Примером таких технологий предотвращения утечек конфиденциальных данных являются DLP–системы. А в борьбе с мошенничеством следует использовать анти–фрод системы, которые предоставляют возможность мониторить, обнаруживать и управлять уровнем фрода.

2.2 Классификация и состав угроз информационной безопасности

На сегодня существует более 100 позиций и разновидностей угроз информационной системе [7]. Угрозы информационной безопасности проявляются не самостоятельно, а через возможное взаимодействие с наиболее слабыми звеньями системы защиты, то есть через факторы уязвимости. Угроза приводит к нарушению деятельности систем на конкретном объекте–носителе.

Основные уязвимости возникают по причине действия следующих факторов:

- несовершенство программного обеспечения, аппаратной платформы;
- разные характеристики строения автоматизированных систем в информационном потоке;
- часть процессов функционирования систем является неполноценной;
- неточность протоколов обмена информацией и интерфейса;
- сложные условия эксплуатации и расположения информации [7].

Чаще всего источники угрозы запускаются с целью получения незаконной выгоды вследствие нанесения ущерба информации. Но возможно и случайное действие угроз из–за недостаточной степени защиты и массового действия угрожающего фактора.

Существует разделение уязвимостей по классам, они могут быть:

- объективными;
- случайными;
- субъективными [14].

Если устранить или как минимум ослабить влияние уязвимостей, можно избежать полноценной угрозы, направленной на систему хранения информации.

Объективные уязвимости

Этот вид напрямую зависит от технического построения оборудования на объекте, требующем защиты, и его характеристик. Полноценное избавление от этих факторов невозможно, но их частичное устранение достигается с помощью инженерно–технических приемов, следующими способами:

1. **Связанные с техническими средствами излучения:**

- электромагнитные методики (побочные варианты излучения и сигналов от кабельных линий, элементов техсредств);
- звуковые варианты (акустические или с добавлением вибросигналов);
- электрические (проскальзывание сигналов в цепочки электрической сети, по наводкам на линии и проводники, по неравномерному распределению тока).

1. **Активизируемые:**

- вредоносные ПО, нелегальные программы, технологические выходы из программ, что объединяется термином «программные закладки»;
- закладки аппаратуры – факторы, которые внедряются напрямую в телефонные линии, в электрические сети или просто в помещения.

1. **Те, что создаются особенностями объекта, находящегося под защитой:**

- расположение объекта (видимость и отсутствие контролируемой зоны вокруг объекта информации, наличие вибро– или звукоотражающих элементов вокруг объекта, наличие удаленных элементов объекта);
- организация каналов обмена информацией (применение радиоканалов, аренда частот или использование всеобщих сетей).

1. **Те, что зависят от особенностей элементов–носителей:**

- детали, обладающие электроакустическими модификациями (трансформаторы, телефонные устройства, микрофоны и громкоговорители, катушки индуктивности);
- вещи, подпадающие под влияние электромагнитного поля (носители, микросхемы и другие элементы) [14].

Случайные уязвимости

Эти факторы зависят от непредвиденных обстоятельств и особенностей окружения информационной среды. Их практически невозможно предугадать в информационном пространстве, но важно быть готовым к их быстрому устранению. Устранить такие неполадки можно с помощью проведения инженерно–технического разбирательства и ответного удара, нанесенного угрозе информационной безопасности:

1. Сбои и отказы работы систем:

- вследствие неисправности технических средств на разных уровнях обработки и хранения информации (в том числе и тех, что отвечают за работоспособность системы и за контроль доступа к ней);
- неисправности и устаревания отдельных элементов (размагничивание носителей данных, таких как дискеты, кабели, соединительные линии и микросхемы);

- сбои разного программного обеспечения, которое поддерживает все звенья в цепи хранения и обработки информации (антивирусы, прикладные и сервисные программы);
- перебои в работе вспомогательного оборудования информационных систем (неполадки на уровне электропередачи).

1. Ослабляющие информационную безопасность факторы:

- повреждение коммуникаций вроде водоснабжения или электроснабжения, а также вентиляции, канализации;
- неисправности в работе ограждающих устройств (заборы, перекрытия в здании, корпуса оборудования, где хранится информация) [14].

Субъективные уязвимости

Этот подвид в большинстве случаев представляет собой результат неправильных действий сотрудников на уровне разработки систем хранения и защиты информации. Поэтому устранение таких факторов возможно при помощи методик с использованием аппаратуры и ПО:

1. Неточности и грубые ошибки, нарушающие информационную безопасность:

- на этапе загрузки готового программного обеспечения или предварительной разработки алгоритмов, а также в момент его использования (возможно во время ежедневной эксплуатации, во время ввода данных);
- на этапе управления программами и информационными системами (сложности в процессе обучения работе с системой, настройки сервисов в индивидуальном порядке, во время манипуляций с потоками информации);
- во время пользования технической аппаратурой (на этапе включения или выключения, эксплуатации устройств для передачи или получения информации).

1. Нарушения работы систем в информационном пространстве:

- режима защиты личных данных (проблему создают уволенные работники или действующие сотрудники в нерабочее время, они получают несанкционированный доступ к системе);
- режима сохранности и защищенности (во время получения доступа на объект или к техническим устройствам);

- во время работы с техустройствами (возможны нарушения в энергосбережении или обеспечении техники);
- во время работы с данными (преобразование информации, ее сохранение, поиск и уничтожение данных, устранение брака и неточностей) [14].

Соответственно различиям в уязвимостях информационной безопасности, существуют и различные классификации угроз информационной безопасности. Каждый из видов таких угроз обладает определенным составом, призванным нарушить состояние безопасности информации. Знание возможных угроз, а также уязвимых мест защиты, которые эти угрозы обычно эксплуатируют, необходимо для того, чтобы выбирать наиболее экономичные средства обеспечения безопасности.

Имеет смысл различать неумышленные и умышленные угрозы.

Неумышленные угрозы связаны с:

- ошибками оборудования или программного обеспечения: сбои процессора, питания, нечитаемые дискеты, ошибки в коммуникациях, ошибки в программах;
- ошибками человека: некорректный ввод, неправильная монтировка дисков, запуск неправильных программ, потеря дисков, пересылка данных по неверному адресу;
- форс–мажорными обстоятельствами.

Умышленные угрозы, в отличие от случайных, преследуют цель нанесения ущерба пользователям информационных систем и, в свою очередь, подразделяются на активные и пассивные. Пассивная угроза – несанкционированный доступ к информации без изменения состояния системы, активная – связана с попытками перехвата и изменения информации.

Еще один из вариантов классификации может быть выполнен по следующим признакам:

- по цели реализации;
- по принципу воздействия на систему;
- по характеру воздействия на систему;
- по причине появления используемой ошибки защиты;
- по способу воздействия атаки на объект;
- по объекту атаки;

- по используемым средствам атаки;
- по состоянию объекта атаки [10].

К наиболее распространенным угрозам безопасности относят:

Несанкционированный доступ (НСД) – наиболее распространенный вид компьютерных нарушений. Он заключается в получении пользователем доступа к ресурсу, на который у него нет разрешения в соответствии с принятой в организации политикой безопасности [4].

Отказ в услуге. Представляет собой преднамеренную блокировку легального доступа к информации и другим ресурсам.

Незаконное использование привилегий. Злоумышленники, применяющие данный способ атаки, обычно используют штатное программное обеспечение, функционирующее в нештатном режиме. Незаконный захват привилегий возможен либо при наличии ошибок в самой системе, либо в случае халатности при управлении системой. Строгое соблюдение правил управления системой защиты, соблюдение принципа минимума привилегий позволяет избежать таких нарушений.

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

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

«Сборка мусора». После окончания работы обрабатываемая информация не всегда полностью удаляется из памяти ПК. Данные хранятся на носителе до перезаписи или уничтожения; при выполнении этих действий на освободившемся пространстве диска находятся их остатки. При искажении заголовка файла их прочитать трудно, но все же возможно с помощью специальных программ и оборудования. Такой процесс принято называть «сборкой мусора». Он может привести к утечке важной информации.

«Люки». Представляют собой скрытую, недокументированную точку входа в программный модуль. «Люки» относятся к категории угроз, возникающих вследствие ошибок реализации какого–либо проекта (системы в целом, комплекса программ и т. д.). Поэтому в большинстве случаев обнаружение «люков» – результат случайного поиска [4].

Вредоносные программы. В последнее время участились случаи воздействия на вычислительную систему специально созданными программами. Для обозначения всех программ такого рода был предложен термин «вредоносные программы». Эти программы прямо или косвенно дезорганизуют процесс обработки информации или способствуют утечке или искажению информации. К самым распространенным видам подобных программ относятся:

- «Вирус»– это программа, которая способна заражать другие программы, модифицируя их так, чтобы они включали в себя копию вируса.
- «Троянский конь» – программа, которая содержит скрытый или явный программный код, при исполнении которого нарушается функционирование системы безопасности. «Троянские кони» способны раскрыть, изменить или уничтожить данные или файлы. Их встраивают в программы широкого пользования, например, в программы обслуживания сети, электронной почты.
- «Червяк» – программа, распространяемая в системах и сетях по линиям связи. Такие программы подобны вирусам: заражают другие программы, а отличаются от вирусов тем, что не способны самовоспроизводиться.
- «Жадная» программа – программа, которая захватывает (монополизирует) отдельные ресурсы вычислительной системы, не давая другим программам возможности их использовать.
- «Бактерия» – программа, которая делает копии самой себя и становится паразитом, перегружая память ПК и процессор.
- «Логическая бомба»– программа, приводящая к повреждению файлов или компьютеров (от искажения данных – до полного уничтожения данных). «Логическую бомбу» вставляют, как правило, во время разработки программы, а срабатывает она при выполнении некоторого условия (время, дата, ввода кодового слова).
- «Лазейки» – точка входа в программу, благодаря которой открывается доступ к некоторым системным функциям. Обнаруживается путем анализа работы программы [9].

Также к классу вредоносных программ можно отнести снифферы (программы, перехватывающие сетевые пакеты), программы подбора паролей, атаки на

переполнение буфера, в некоторых приложениях – дизассемблеры и отладчики [9].

Во второй главе работы рассмотрено понятие угрозы информационной безопасности. Нельзя сказать, что информация находится в состоянии безопасности, если ей что-либо угрожает. В связи с этим были названы и проанализированы уязвимости в различных системах, упорядочивающих информацию. И уже исходя из выделенных уязвимостей выделены и виды угроз информационной безопасности. Следует отметить, что реализация того или иного вида угрозы информационной безопасности, как правило, является закономерной – каждая случайная или специальная угроза реализуется в том месте системы, которое наиболее уязвимо. В связи с этим можно сделать вывод, что своевременная профилактика позволит свести к минимуму число инцидентов информационной безопасности, и, кроме того, минимизировать последствия от все-таки реализованных угроз. Здесь также важно, что профилактика реализации угроз информационной безопасности возможна не только на крупных коммерческих и государственных предприятиях, но и на частных компьютерах, что позволит сохранить тайну личной жизни.

Заключение

В ходе выполнения работы была достигнута цель исследования: изучены виды и состав угроз информационной безопасности.

Для достижения данной цели были выполнены следующие задачи:

- рассмотрены понятие и сущность информации;
- проанализирована суть информационной безопасности;
- охарактеризовано понятие угрозы информационной безопасности;
- рассмотрена классификация и состав угроз информационной безопасности.

Угрозы информационной безопасности на сегодняшний день актуальны, как никогда ранее. Из изученного материала становится очевидно, что угрозы информационной безопасности различаются по огромному числу видов и по составу. Примечательно, что угрозы информационной безопасности и средства их реализации модифицируются, множатся и разрастаются с пугающе высокой скоростью.

Кроме того, в ходе выполнения работы было определено, что вид угрозы информационной безопасности, которая была применена или может быть применена, зависит от того, какие виды уязвимостей характерны той или иной информационной системе. Также важно, что подавляющее число таких уязвимостей может быть выявлено и своевременно устранено/усилено, благодаря чему появится возможность минимизации последствий от реализации угроз информационной безопасности, либо их избегания совсем.

Текст работы может быть дополнен и модернизирован согласно требованиям времени. Так как информации становится все больше, а средства защиты и, наоборот, угрозы для нее модернизируются и развиваются, вопрос еще долго нельзя будет назвать изученным полностью.

Список использованной литературы

1. ГОСТ Р 50922-96 Защита информации. Основные термины и определения [Электронный ресурс]. Режим доступа: http://docs.cntd.ru/document/1200004674
2. Бабаш А. В. Информационная безопасность (+ CD–ROM) / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. – М.: КноРус, 2013. – 136 с.
3. Бачило И. Л. Информационное право: Учебник / И. Л. Бачило; Под ред. Акад. РАН Б.Н. Топорникова. – СПб.: Издательство «Юридический центр Пресс», 2016.
4. Васильков А. В. Безопасность и управление доступом в информационных системах / А. В. Васильков, И. А. Васильков. – М.: Форум, 2015. – 368 с.
5. Галатенко В. А. Основы информационной безопасности: учебное пособие / В. А. Галатенко; под ред. академика РАН В. Б. Бетелина, – 4–е изд. – М.: Интернет–Университет Информационных технологий; БИНОМ. Лаборатория знаний, 2018. – 205 с.
6. Галатенко В. А. Стандарты информационной безопасности. Курс лекций / В. А. Галатенко. – М.: ИНТУИТ.РУ Интернет–университет Информационных Технологий, 2016. 264 с.
7. Гафнер В. В. Информационная безопасность / В. В. Гафнер. – М.: Феникс, 2014. – 336 с.
8. Гришина Н. В. Информационная безопасность предприятия. Учебное пособие / Н. В. Гришина. – М.: Форум, 2015. – 240 с.
9. Девянин П. Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах / П. Н. Девянин. – М.: Радио и связь, 2013. – 176 с.

10. Кисляков П. А. Информационная безопасность / П. А. Кисляков, С. В. Петров. – Москва: СПб. [и др.] : Питер, 2013. – 329 с.
11. Мельников В. В. Безопасность информации в автоматизированных системах / В. В. Мельников. – М.: Финансы и статистика, 2015. – 368с.
12. Мельников В. В. Информационная безопасность / В. В, Мельников, С. А. Клейменов, А. М. Петраков. – М.: Академия, 2015. – 336с.
13. Мельников В. П. Информационная безопасность / В. П. Мельников, С. А. Клейменов, А. М. Петраков. – М.: Academia, 2017. – 336 с.
14. Партыка Т. Л. Информационная безопасность / Т. Л. Партыка, И. И. Попов. – М.: Форум, Инфра–М, 2016. – 368 с.
15. Ярочкин В. И. Информационная безопасность/ В. И. Ярочкин. – М.: Гаудеамус, 2014. – 544с.
16. Ященко В. В. Введение в криптографию / Под общей ред. В. В. Ященко. – СПб.: Питер, 2015. – 288 с.