Содержание:

ВВЕДЕНИЕ

Актуальность работы. В современных условиях информационной эры XXI века информационная безопасность приобретает все более весомую роль, а вопрос ее обеспечения становятся все острее. Стремительное внедрение информационных, компьютерных технологий во все сферы жизнедеятельности общества и развитие экономики актуализирует вопрос определения обоснованных и эффективных путей обеспечения информационной безопасности.

Процессы комплексной информатизации развития страны обусловливают активное воздействие информационной безопасности на экономическую, социальную, политическую и другие составные ее национальной безопасности. В научных трудах отечественных и зарубежных ученых-экономистов представлены многочисленные исследования информационной безопасности [2-7]. Однако вопрос построения эффективной политики обеспечения информационной безопасности остаются все еще малоизученными.

Целью работы является рассмотрение видов и состава угроз информационной безопасности.

Объект исследования: информационная безопасность.

Предмет исследования: особенности угроз информационной безопасности.

Для осуществления поставленной цели необходимо решить задачи:

- рассмотреть сущность информационной безопасности;

- раскрыть виды угроз информационной безопасности РФ;

- указать состав угроз информационной безопасности.

Глава 1. Характеристика информационной безопасности

1.1. Сущность информационной безопасности

Динамичное развитие экономических, политических, социальных событий XXI века сформулировали новое представление об информации как одного из факторов (ресурсов) производства.

На макроуровне информация уверенно занимает позиции главного фактора мощи государства, ведь способность государства располагать современные информационные технологии позволяет эффективно управлять информацией. Знание государством такой способностью - путь к дальнейшему наращиванию своей экономической и военной прочности [3].

На микроуровне объем, достоверность, целостность, качество обработки информации определяет эффективность действий менеджмента предприятия, а, следовательно, актуализирует использование информационных технологий в управлении денежно-кредитными, финансовыми, социально-экономическими процессами данного предприятия. «Без необходимого объема и качества информации невозможно обеспечить развитие предприятия на основе высокотехнологичного производства, эффективных методов организации труда» [7].

На сегодняшний день существует много подходов к определению термина «информация». Так, например:

- информация - это документированные или публичные сведения о событиях и явлениях, происходящих в обществе, государстве и окружающей среде [8];
- информация - представляет собой результат отражения и обработки в человеческом сознании многообразия окружающего мира, сведений о предметах, окружающих человека, явления природы, деятельность других людей и т. п. [5].

Глобальные процессы информатизации общества государств мира и широкое внедрение информационных технологий (как характерные черты нынешнего века), их влияние на все сферы развития этих государств, выдвигает на первый план вопросы обеспечения информационной безопасности. От взвешенной политики информационной безопасности, от степени защищенности, полноты и достоверности информации в современном мире зависит стабильность социально-экономической ситуации государства, сохранения правопорядка, обеспечения прав

ее граждан.

Попробуем проанализировать терминологию по информационной безопасности. Основные определения сущности информационной безопасности указано в многочисленных нормативно-правовых актах центральных органов законодательной и исполнительной власти.

Многочисленные исследователи предлагают следующие мнения относительно рассматриваемого термина:

- под информационной безопасностью предприятия предлагаем понимать общественные отношения по созданию и поддержанию на должном уровне жизнедеятельности информационной системы субъекта хозяйственной деятельности [7];
- информационная безопасность - состояние информации, при котором обеспечивается сохранение определенных политикой безопасности свойств информации [1];
- информационная безопасность - это состояние защищенности информационной среды общества, обеспечивает его формирование, использование и развитие в интересах граждан, организаций, государства [1];
- информационная безопасность - представляет собой состояние защищенности потребностей в информации личности, общества и государства, при котором обеспечивается их существование и прогрессивное развитие независимо от наличия внутренних и внешних информационных угроз [2];
- под информационной безопасностью следует понимать одну из сторон рассмотрения информационных отношений в рамках информационного законодательства с позиций защиты жизненно важных интересов личности, общества, государства и акцентирование внимания на угрозах этим интересам и на механизмах устранения или предотвращения таких угроз правовыми методами [1].

Заслуживает отдельного внимания исследования сущности анализируемого термина авторами [4]. Они предлагают выделить следующие три аспекта определения сущности «информационная безопасность»:

1. нормативно-правовой (основывается на анализе нормативно-правовых актов) - рассматривает как неотъемлемую часть политической, экономической, оборонной и других составляющих национальной безопасности [3];

2. доктринальный (исходя из анализа трактовок термина в работах исследователей, специалистов в этой отрасли)

а) при информационной безопасностью понимают состояние правовых норм и соответствующих им институтов безопасности, которые гарантируют постоянное наличие данных для принятия стратегических решений и защита информационных ресурсов страны [5];

б) информационная безопасность - безопасность объекта от информационных угроз или негативных воздействий, связанных с информацией и неразглашение данных о том или ином объекте, составляющих государственную тайну [6];

в) информационная безопасность - это защищенность установленных законом правил, по которым происходят информационные процессы в государстве, обеспечивающих гарантированные Конституцией условия существования и развития человека, всего общества и государства [7];

г) национальная информационная безопасность - это общественные отношения, связанные с защитой жизненно важных интересов человека и гражданина, общества и государства от реальных и потенциальных угроз в информационном пространстве, что является необходимым условием сохранения и приумножения духовных и материальных ценностей нации, прогрессивного развития страны, зависит от целенаправленной информационной политики гарантий, охраны, обороны, защиты ее национальных интересов [8];

3. энциклопедический (в основе - анализ определений, приведенных в словарях, энциклопедиях) - информационная безопасность означает:

а) законодательное формирование государственной информационной политики; обеспечения свободы информационной деятельности и права доступа к информации в национальном информационном пространстве страны; создание и внедрение безопасных информационных технологий;

б) охрану государственной тайны, а также информации с ограниченным доступом;

в) защита национального информационного пространства страны от распространения искаженной или запрещенной для распространения информационной продукции.

Анализ перечисленных подходов к трактовке термина «информационная безопасность» позволяет выделить ее следующие сущностные характеристики

(черты). Итак, информационная безопасность - это:

- состояние защищенности информационного пространства;
- состояние защищенности национальных интересов страны в информационной среде;
- защищенность установленных законом правил, по которым происходят информационные процессы в государстве;
- общественные отношения, связанные с защитой жизненно важных интересов человека и гражданина, общества и государства от реальных и потенциальных угроз в информационном пространстве;
- неотъемлемая часть политической, экономической, оборонной и других составляющих национальной безопасности [4].

Таким образом, информационная безопасность является одной из составляющих устойчивого развития всего государства, а процесс обеспечения информационной безопасности необходимо понимать как: «... одно из глобальных и приоритетных задач органов государственного управления, решению которого должны быть подчинены политическая, экономическая, военная, культурная и другие виды деятельности системы государственного управления» [4].

В процессе исследования информационной безопасности важным вопросом выступает мониторинг угроз и рисков, которые могут угрожать ее эффективности.

Информационные угрозы представляют опасность для индивида, общества и государства. «Реализация угроз и перерастания их в опасности свидетельствует о неэффективности функционирования системы государственного управления информационной безопасностью» [4]. Управление угрозами и опасностями способствует их устранению.

Угрозы информационной безопасности можно трактовать как совокупность внутренних и внешних условий, которые могут нанести ущерб интересам личности и общества через нежелательные информационные атаки на соответствующие об объекты информационной инфраструктуры государства.

Актуальность изучения угроз информационной безопасности подтверждает в своей работе и [6]: «.Учитывая тот факт, что под влиянием информационных атак может целенаправленно изменяться мировоззрение и мораль как отдельных лиц, так и общества в целом, навязываются чужие интересы, мотивы, способ жизни, на первый план следует анализ сущности и форм проявлений современных методов скрытого агрессивного воздействия, проявления действий, имеющих

целенаправленный агрессивный характер и которые противоречат интересам национальной безопасности и выработка механизмов противодействия им во все направлениях ».

Исходя из многочисленных исследований [2-4] можно выделить следующие виды угроз информационной безопасности:

- угрозы воздействия некачественной информации (недостоверной, ложной, дезинформации) на личность, общество, государство;
- угрозы несанкционированного и неправомерного воздействия посторонних лиц на информацию и информационные ресурсы (на производство информации, информационные ресурсы, на системы их формирования и использования);
- сбои в работе оборудования (может возникнуть при блокировании доступа к одному или нескольким ресурсам информационной системы);
- угрозы информационным правам и свободам личности (правую на производство, распространение, поиск, получение, передачу использование информации; праву на интеллектуальную собственность на информацию и материальную собственность на документированную информацию; праву на личную тайну; праву на защиту чести и достоинства и т. д.)

Источники угроз разделяют на три группы:

- первая группа - источники угроз информационной безопасности личности (то есть обеспечению конституционных прав и свобод человека и гражданина на доступ к открытой информации, на использование информации в интересах осуществления не запрещенной законом деятельности, а также в защите информации, обеспечивающей личную безопасность, духовное и интеллектуальное развитие. Пример, существенное расширение возможности манипулирования сознанием человека за счет формирования вокруг нее индивидуального «виртуального информационного пространства», а также возможность использования технологий воздействия на его психическую деятельность);
- вторая группа - источники угроз информационной безопасности общества (непрерывное усложнение информационных систем и сетей связи критически важных инфраструктур обеспечения жизни общества. Пример: умышленные и неумышленные ошибки, сбои и отказы техники и программного обеспечения, вредное воздействие со стороны преступных структур и криминальных элементов, расширение масштабов отечественной и международной

компьютерной преступности, осуществление мошеннических операциях с использованием глобальных или отечественно информационно-телекоммуникационных систем, отмывание финансовых средств, полученных противоправным путем);
- третья группа - источники информационной безопасности государства (получение противоправного доступа к сведениям, составляющим государственную тайну, в другой конфиденциальной информации, раскрытие которой может нанести ущерб государству; попытки реализации концепции ведения информационных войн; неконтролируемое распространение информационного оружия) [1].

Остановимся более подробно на понятии «информационная война». Она представляет собой высшую степень информационного противоборства, направленная на решение общественно-политических, идеологических, национальных, территориальных конфликтов между государствами, народами, нациями и социальными группами путем широкомасштабной реализации средств и методов информационного оружия.

Информационная война включает следующие действия:

1. оказания влияния на телекоммуникации, транспортные сети и тому подобное;
2. промышленный шпионаж (нарушение прав интеллектуальной собственности, проведения конкурентной разведки, хищения патентованной информации);

- хакинг (взлом и использования личных данных, информации с ограниченным доступом) [4].

Информационное оружие является основным инструментом осуществления информационной войны, и представляет собой совокупность средств, методов и технологий, обеспечивающих возможность силового воздействия на информационную сферу противоположной стороны (разрушение ее информационной инфраструктуры, системы управления государством, снижение духовного потенциала общества).

Среди наиболее серьезных задач, которые могут решаться с помощью современного информационного оружия, можно отметить:

- создание атмосферы бездуховности и безнравственности;
- манипулирования общественным сознанием и политической ориентацией социальных групп населения государства с целью создания политической

напряженности и хаоса;
- дестабилизация политических отношений между партиями, объединениями и движениями с целью провокации конфликтов, разжигание недоверия, обострение политической борьбы;
- дезинформация населения о работе государственных органов, подрыв их авторитета, дискредитация органов управления;
- провоцирование социальных, политических, национальных и религиозных столкновений и т.д. [11].

Изучение разрушительного воздействия угроз информационной безопасности выдвигает на первое место вопросы построения эффективной системы ее обеспечения. В современном мире обеспечение информационной безопасности должно выступать одной из важнейших функций государства.

Содержание, порядок реализации обеспечения информационной безопасности, инструменты, задачи и нормативное регулирование этого процесса заключаются в следующем:

- Информационная безопасность обеспечивается проведением единой государственной политики национальной безопасности в информационной сфере.
- Инструментом реализации государственной политики информационной безопасности выступает система обеспечения информационной безопасности. Последняя собой представляет организационное сочетание мероприятий (информационного, административного, управленческого, методологического характера), направленных на обеспечение информационной безопасности личности, общества и государства.

Задачами системы обеспечения информационной безопасности являются:

мониторинг, прогнозирование реализации дестабилизирующих факторов и информационных угроз жизненно важным интересам личности, общества и государства;

осуществление комплекса оперативных и долговременных мер по их предупреждению и устранению;

создание и поддержание в готовности сил и средств обеспечения информационной безопасности;

совершенствования государственной политики развития информационной сферы (создание благоприятных условий развития национальной информационной инфраструктуры, внедрение новейших технологий в этой сфере);

обеспечение информационно-аналитического потенциала страны.

Итак, информационная безопасность имеет одно из первоочередных значений для социально-экономического развития государства.

Россия должна продолжить активные шаги на пути развития собственной системы информационной безопасности. Важными мерами в этом процессе должны стать организация и проведение информационных операций, а также развитие системы сертификации информационных продуктов. Кроме того, система обеспечения информационной безопасности должна гибко корректироваться в соответствии с изменяющимся характером внешних и внутренних факторов окружения.

1.2. Выявление угроз информационной безопасности

Угрозы информационной безопасности по своей актуальности занимают второе место среди основных угроз бизнеса, таких как экономическая нестабильность, промышленный шпионаж, хищение интеллектуальной собственности, нанесения вреда репутации и тому подобное.

Такой вывод сделали эксперты по результатам совместного исследования «Информационная безопасность бизнеса, 2015» [12], которое в 2015 году было проведено в 22 странах мира известной в области информационной безопасности российской компанией «Лаборатория Касперского» совместно с компанией B2B International (Великобритания), специализируется на проведении исследований для бизнеса по широкому кругу вопросов.

При этом в отчете говорится, что нет оснований говорить об уменьшении уровня угроз информационной безопасности в ближайшее время. Напротив, эксперты ожидают роста интенсивности угроз, повышение уровня их технического сопровождения и возникновения новых.

Такое положение дел не может не вызвать интереса экспертов в области информационной безопасности. Ведущие мировые компании и учреждения в

области информационной безопасности и безопасности государства в течение последних лет периодически проводили исследования защищенности информационных систем, в том числе и с точки зрения несанкционированной утечки информации.

Среди них, например, совместные исследования ФБР и Института компьютерной безопасности CSI (США) «Computer Crime and Security Survey», исследование компании Ernst & Young «Global Information Security Survey, исследования российских ком дам InfoWatch и Лаборатории Касперского [13], периодические исследования компании Perimetrix «Персональные данные в России» [14] и ряд других исследований. Приведенные исследования проводились путем анкетирования экспертов в области информационной безопасности и управления бизнесом и анализа анкет опроса.

В качестве экспертов привлекались сотрудники различных по величине и объему услуг компаний в различных отраслях хозяйства из разных стран мира, работа которых связана с вопросами информационной безопасности, ИТ - технологиями и управлением учреждениями и организациями.

С точки зрения неконтролируемой утечки данных за периметр информационных систем, заслуживает внимания исследование «Глобальное исследование утечек корпоративной информации и конфиденциальных данных» [15], которые периодически проводились в течение последних лет компанией InfoWatch.

Методика таких исследований отличается от методик предварительно приведенных исследований тем, что анализировались не точки зрения экспертов по тем или иным вопросам информационной безопасности, а зафиксированные и обнародованы в общедоступных средствах информации (СМИ, Internet и т.д.) случаи неконтролируемой утечки информации за периметр информационных систем. В данном исследовании анализировались инциденты по информационной безопасности, связанные исключительно с утечкой данных. В него не вошли, но не анализировались данные об инцидентах, связанных с внешними угрозами информационной безопасности (вирусы, внешние компьютерные атаки, DDoS, фишинг и прочее).

Иными словами, исследование касается исключительно проблемы утечки информации за пределы защищенных информационных систем учреждений и организаций по тем или иным причинам. При этом результаты исследований, проведенных по различным методикам, не противоречат друг другу и, в основном,

совпадают. Это дает право воспользоваться ими для выявления тенденций развития угроз информационной безопасности, их характера и интенсивности возникновения, а также оценить результаты, полученные от внедрения тех или иных методов и систем противодействия угрозам.

Как известно, современные технологии обработки информации, и персональных данных в том числе, предусматривают использование ИС [16, 17]. Такие системы представляют собой взаимосвязанную совокупность средств, методов и персонала, обеспечивающих сбор, хранение, обработку, передачу и воспроизведение информации с целью достижения поставленной цели.

Информация является центральным компонентом ИС. При этом объектами защиты становятся информационная система, в которой обрабатывается информация с использованием определенных информационных технологий, информационные технологии и, собственно, сама информация.

Среди угроз информационной безопасности выделяют две группы угроз: внутренние и внешние [18].

К внешним угрозам относятся угрозы, которые возникают и управляемых вне ИС, относительно ресурсов, которых они направлены.

Внутренние угрозы возникают непосредственно в пределах ИС. Они могут поступать от технического оборудования, несовершенных программных средств и персонала.

Как показывают проведенные исследования, противодействия угрозам информационной безопасности уделяется определенное внимание со стороны операторов ИС. Практически все операторы внедрили в состав ИС средства противодействия как внутренним, так и внешним угрозам.

Так сложилось, что противодействия внешним угрозам уделялось больше внимания, чем противодействия внутренним угрозам. Периметр информационной системы защищался в большей степени, чем минимизировали внутренние угрозы. Поэтому на сегодняшний день средства противодействия внешним угрозам внедрены более широко, чем средства противодействия внутренним угрозам.

Путем внедрения мер противодействия угрозам информационной безопасности операторы ИС достигли определенного уровня защиты их отдельных компонентов и ИС в целом от внешних угроз информационной безопасности. Такие

информационные системы называют защищенными [17] и, с определенным уровнем вероятности, можно утверждать, что информация, прорабатывается такими системами, в их пределах, защищена от внешних угроз. При этом острым остается вопрос противодействия внутренним угрозам информационной безопасности, актуальность которого растет.

Так, если по результатам исследования «Information security breaches survey 2006», проведенного международной компанией Price Waterhouse Coopers в 2006 году, считали актуальными вопросы противодействия внутренним угрозам информационной безопасности 32% экспертов в области информационной безопасности и безопасности бизнеса, то в 2011 году эксперты из ФБР и Института компьютерной безопасности CSI (США), по результатам исследования «Computer Crime and Security Survey 2010/2011», проведенного с той же аудиторией экспертов, признали проблему противодействия внутренним угрозам информационной безопасности в качестве приоритетной. Минимизировать такие угрозы можно путем внедрения систем противодействия внутренним угрозам информационной безопасности.

Известны четыре класса таких систем.

Среди них:

- системы мониторинга и аудита;
- системы аутентификации;
- средства шифрования;
- системы обнаружения и предупреждения утечки информации.

Система мониторинга и аудита позволяют регистрировать действия пользователей и процессов в ИС, в том числе действия и процессы, связанные с пересылкой данных за пределы ИС сетевыми каналами.

Такие системы являются важным средством при расследовании зафиксированных случаев несанкционированной утечки информации, за периметр защищенных ИС и проведении их анализа.

Недостатком таких систем является отсутствие возможности предупреждения несанкционированной утечки информации. В работе систем мониторинга и аудита не предусмотрены алгоритмы проведения анализа зафиксированных событий.

Это значит, что они не могут определить, зафиксированное событие допустимое с точки зрения информационной безопасности или нет. Закономерно, что в таких системах непредвиденные любые алгоритмы блокировки передачи данных сетевыми каналами.

Системы аутентификации пользователей ИС применяются для защиты от несанкционированного доступа к данным. В их основе лежит процесс аутентификации пользователя (может быть двух - или три этапный). По его результатам пользователю может быть либо предоставлен доступ к приглашенным ресурсам, либо нет, чем предупреждается о возможной несанкционированной утечки информации за пределы ИС.

Такие средства не могут защитить информацию от пользователя, который по нормам политики безопасности ИС имеет доступ к данным, но при этом планирует использовать их в целях, противоречащих нормам действующего законодательства или политике безопасности компании (от инсайдера).

Средства шифрования носителей меняют данные таким образом, что ими невозможно воспользоваться без специальных программ (ключей). Этот класс программ защитит данные от утечки при потере мобильной системы хранения или обработки информации и при перехвате данных злоумышленником за пределами защищенной ИС.

Эффективность такого средства защиты нивелируется, если вместе с данными к злоумышленнику попадут ключи шифрования.

Системы обнаружения и предупреждения утечки информации (Data Leakage Prevention, DLP-системы) проводят сканирование возможных каналов утечки данных в реальном масштабе времени, а также могут контролировать действия пользователей и процессы обработки и передачи информации в пределах ИС. При этом такие системы способны распознавать информацию по определенным категориям. Они могут быть комплексными или локальными. Комплексные DLP-системы контролируют несколько каналов утечки информации. Например, копирование на мобильные носители, системы печати, сетевые каналы передачи информации и тому подобное.

Локальные системы контролируют лишь один из возможных каналов утечки информации, чаще всего сетевой. В таких системах могут быть внедрены активные технологии, благодаря которым появляется возможность не только выявлять случаи несанкционированного перемещения информации за периметр

защищенных ИС, но и блокировать их. Дополнительной функцией DLP-систем может быть шифрования данных в процессе записи на носителе или в файлы.

Существуют и другие программно-аппаратные средства защиты информации от внутренних угроз информационной безопасности, которые нельзя непосредственно отнести к приведенным выше категорий. Например, средства блокировки внешних носителей информации. Такие системы не могут распознавать информацию по категориям, не отличают информацию ограниченного распространения от общего и является реализацией отдельных функций приведенных систем защиты от внутренних угроз.

На сегодняшний день только системы обнаружения и предупреждения утечек информации (DLP-системы) является единственным решением, позволяющим предотвратить утечки информации за пределы защищенного пространства ИС в реальном масштабе времени на основе фильтрации данных или внешних атрибутов, сопровождающих процесс перемещения данных. Обычно ядро подобных DLP систем составляют технологии категоризации контента, основанные на контейнерном или контекстном анализе исходного потока. Преимущества контейнерного анализа заключаются в простоте его реализации, к недостаткам относят организационные трудности при внедрении и ограниченные возможности контроля исходящего трафика.

Каждый из приведенных методов имеет свои преимущества и недостатки. Преимущества лингвистических технологий состоит в том, что они работают непосредственно с содержанием документов, могут самосовершенствоваться, их быстродействие напрямую зависит от объема потока информации, к недостаткам относят зависимость от языка сообщения низкую эффективность при анализе структурированной информации, медийных и графических файлов.

Статистические методы воспринимают файл как последовательность символов, поэтому эффективно работают с текстовыми документами на разных языках, а также с медийными и графическими файлами. К недостаткам статистических методов относят, возможен высокий процент ложных срабатываний и трудоемкий процесс отладки системы.

Существует две архитектуры DLP систем: шлюзов или хостов.

Преимущества шлюзовых систем заключаются в простоте реализации.

К недостаткам относят ограниченную область применения и проблемность анализа некоторых видов трафика, например семейства SSL.

К преимуществам хостовых систем относят более широкий круг возможностей контроля за утечкой данных, в том числе и несетевыми каналами.

Можно предположить, что сочетание методов контекстной и контентной фильтрации данных может быть основой для создания эффективной системы выявления и предупреждения несанкционированной утечки ПД сетевыми каналами.

Глава 2. Характеристика видов и состава угроз информационной безопасности

2.1. Виды угроз

Угроза раскрытия информационных ресурсов заключается в том, что данные, знания и информация делаются известными тем, кому не следует их знать. Под угрозой раскрытия понимается такое состояние, когда полученный несанкционированный доступ к ресурсам системы, причем речь идет как о открытые, и те ресурсы, которые имеют ограниченный доступ. Эти ресурсы обязаны передаваться друг другу и храниться в единой информационной системе.

Угроза сбоя в работе самого оборудования может появится при блокировании доступа к одному или нескольким ресурсам информационной системы. Блокирование может быть постоянным, так чтобы запрашиваемый ресурс никогда не был получен, или может создать задержания в получении ресурса, спрашивается, что является достаточным для того, чтобы он стал бесполезным.

Теория и практика свидетельствует о существовании двух групп угроз по информационной безопасности предприятия, таких как неспециальные или случайные действия, выражающиеся в неадекватной поддержке механизмов защиты и ошибках в управлении, и преднамеренные угрозы - несанкционированный доступ к информации и несанкционированные манипуляция данным, ресурсами и самыми системами.

Также классификация угроз информационной безопасности может быть осуществлена разделением угроз на связанные с внутренними и внешними факторами. Отдельно стоит выделить угрозы, связанные с преднамеренными ошибками, возникающими за пределами бизнеса.

К таким угрозам относятся:

- несанкционированный доступ к информации, хранящейся в системе;

- отрицание действий, связанных с манипулированием информации (например, несанкционированное изменение, которая ведет к нарушению целостности данных);

- введение в программные продукты и проекты «логических бомб», которые срабатывают при выполнении определенных условий или по истечении определенного периода времени и частично или полностью выводят из строя компьютерную систему;

- разработка и распространение компьютерных вирусов;

- небрежность в разработке, поддержке и эксплуатации программного обеспечения, приводит к краху компьютерной системы;

- изменение компьютерной информации и подделка электронных подписей; -

хищение информации с последующим маскировкой;

- перехват информационных потоков;

- отрицание действий или услуги;

- отказ в предоставлении услуги.

К сожалению, приходится констатировать, что унифицированный подход к классификации угроз информационной безопасности отсутствует. И это вполне понятно, так как при всем том многообразии информационных систем, направленных на автоматизацию множества технологических процессов, затрагивающих различные сферы человеческой деятельности, жесткая систематизация и классификация угроз неприемлема.

Можно предложить такую классификацию угроз:

- за проявлением и последствиями

преступление; мошенничество;

хулиганство.

- по типу

программное; аппаратное, прочее.

- За целью - оперативные, тактические, стратегические.

- По характеру возникновения - преднамеренные, непреднамеренные. -

За информационными технологиями - объект угроз, методы подготовки угроз, инструментарий угроз, среда угроз.

- по месту возникновения - инсайдерские, внешние.

- За объектом воздействия - системные, локальные.

- По причине возникновения - сбои в оборудовании, сбои в работе программного обеспечения, несовершенная архивация данных, несанкционированный доступ.

Проанализируем виды угроз более детально.

По источникам происхождения:

техногенного происхождения - транспортные аварии (катастрофы), пожара, неспровоцированные взрывы или их угроза, аварии на инженерных сетях и сооружениях жизнеобеспечения, внезапное разрушение каналов связи, аварии главных серверов органов государственного управления и т.д.;

природного происхождения - включают в себя опасные метеорологические, геологические, гидрологические морские и пресноводные явления, природные пожары, деградацию почв недр, массовое поражение сельскохозяйственных растений и животных болезнями или вредителями, изменение состояния водных ресурсов и биосферы и тому подобное;

антропогенного происхождения - совершение человеком разных действий по разрушению информационных ресурсов, систем, программного обеспечения объекта и тому подобное.

К этой группе по содержанию действий относятся: непреднамеренные, вызванные непреднамеренными или ошибочными действиями человека (это, например, может быть ложный запуск программы, нечаянно инсталляция закладок и т.п.); преднамеренные (инспирированы), ставшие итогом преднамеренных действий людей (например: намеренное введение вирусов, умышленное инсталляция программ, которые передают информацию на другие компьютеры и т.д.).

По степени гипотетической вреда:

угрозы явные или потенциальные действия, которые делают невозможным или затрудняют реализацию национальных интересов в информационной сфере и воссоздают опасность для системы государственного управления, жизнеобеспечения ее системообразующих элементов;

опасность - непосредственная дестабилизация функционирования системы государственного управления.

По повторяемости совершения:

продолжающиеся - неоднократное выполнение угроз, состоящий из ряда совокупных, которые имеют общую цель.

повторяющиеся - такие угрозы, которые уже ранее имели место;

По сферам происхождения:

эндогенные - алгоритм дестабилизации системы размещен в самой системе;

экзогенные - источник дестабилизации системы находится за ее пределами.

По вероятности реализации:

невозможны - такие угрозы, за осуществление некоторого комплекса условий никогда не состоятся. Такие угрозы обычно имеют значительный декларативный характер, не подкрепленный реальной и даже потенциальной возможностью осуществить провозглашенные намерения, они в основном имеют запугивающий характер;

вероятные - такие угрозы, за осуществление некоторого комплекса условий обязательно состоятся. Примером может быть объявление атаки информационных ресурсов субъекта обеспечения национальной безопасности, которое предшествует самой атаке;

случайные - такие угрозы, за осуществление некоторого комплекса условий каждый раз протекает по-разному. Угрозы такого уровня правильно анализировать с помощью методов исследования операций, в особенности теории вероятностей и теории игр, которые изучают закономерности в случайных явлениях.

По уровню детерминизма:

случайные - такие угрозы, которые могут или не случиться, либо случиться;

закономерные - такие угрозы, которые носят повторяющийся, устойчивый характер, вызванный объективными условиями развития и существования системы информационной безопасности. Так, например, любой субъект ЗНБ будет подвергаться информационным атакам, если в нем не работает, или работает не на должном уровне система обеспечения информационной безопасности;

По значению:

допустимые - такие угрозы, которые не могут создать к коллапсу системы. Примером могут быть вирусы, не повреждают программы путем их уничтожения;

недопустимы - такие угрозы, которые:

1) могут в случае их применения привести к системной дестабилизации системы и коллапсу;

2) могут привести к изменениям, не совместимых с последующим существованием СНБ. Так, например, вирус "I love you", вызвал повреждения компьютерных систем во многих городах мира, и нанес общий ущерб около 100 000 000 долларов США.

По структуре воздействия:

структурные - угрозы, которые влияют на отдельные структуры системы. Такие угрозы также опасны, одновременно они касаются структуры отдельных органов государственной власти или их компонентов;

системные - угрозы, влияющие сразу на все составляющие элементы субъекта ЗНБ. Это влияние обязано осуществляться одновременно в нескольких наиболее важных и уязвимых местах. Для субъекта ЗНБ это может быть целенаправленная дискредитация их работников через радиовещание, телевидение, Интернет, печатные средства массовой информации.

элементные - угрозы, влияющие на отдельные элементы структуры системы. Такие угрозы носят постоянный характер и могут быть опасными только при условии неоправданного или неэффективности их мониторинга. Так, например, в свое время, в конце 60 годов XX века, когда в Италии действовали так называемые "Красные бригады", власть не уделяла большого внимания действиям террористов, которые сначала угрожали, а затем начали физически ликвидировать всех судей, которые выносили обвинительные приговоры террористам. Жертвой неадекватной и халатности оценки информационной угрозы стал и на то время экс премьер-министр Италии Альдо Моро, который был предупрежден заранее о нападении, одновременно власти не приняли соответствующих мер и он был похищен, а затем и убит. Тоже самое относится к событиям с совершением актов терроризма 11 сентября 2001 года.

По характеру реализации:

потенциальные - активизация алгоритмов дестабилизации возможна при некоторых условиях среды функционирования органа государственного управления;

реальные - активизация алгоритмов дестабилизации считается неизбежной и не ограничена пространственной действием и временным интервалом;

мнимые - псевдоактивизация алгоритмов дестабилизации, или активизация таких алгоритмов, по некоторым признакам схожи с методами дестабилизации, но таковыми не являются;

осуществлены - такие угрозы, которые воплощены в жизнь.

По отношению к ним:

субъективные - множество факторов объективной действительности, которая считается субъектом управления системой безопасности угрозой. При таком случае значимую роль в определении тех или иных факторов и обстоятельств играет воля субъекта управления, и принимает непосредственное решение о предоставлении статуса или идентификации тех или других событий в качестве угроз безопасности.

объективные - такие угрозы, которые подтверждаются совокупностью фактов и обстоятельств, объективно характеризующих окружающую среду;

По объекту воздействия:

на человека;

на государство;

на общество.

По формам закрепления:

ненормативные - существуют объективно, но не считаются осознанными высшим политическим руководством государства и не нашли адекватного отражения в нормативной системе государства;

нормативные - официально признаны и осознанные как в нормативных актах страны.

Таким образом, перечисленные виды угроз информационной защиты не дают полного представления о составе угроз информационной защиты, поэтому данный вопрос необходимо рассмотреть в следующем разделе.

2.2. Состав угроз защищаемой информации

Есть три разных подхода в идентификации угроз, которые включают в себя следующее:

1. угроза трактуется как явление (случай, событие или возможность их появление), результатом которых могут быть нежелательные воздействия на информацию;
2. угроза рассматривается как потенциально существующая ситуация (опасность, возможность) нарушения безопасности информации, при этом безопасность информации подразумевает, что информация находится в таком защищённом виде, которая способна противостоять любым дестабилизирующим воздействиям;
3. угроза определяется как потенциально возможные или реальные действия, или условия, приводящие к той или иной форме проявления уязвимости информации.

Любая угроза не сводится к чему-то однозначному, она состоит из некоторых взаимосвязанных компонентов, каждый из которых сам по себе не представляет угрозу, но является её частью. Сама угроза появляется только при совокупном их

взаимодействии.

Угрозы защищаемой информации связаны с её уязвимостью, то есть неспособностью информации самостоятельно противостоять дестабилизирующим воздействиям, нарушающим её статус. А нарушение статуса защищаемой информации состоит в нарушении её физической сохранности, доступности для правомочных пользователей, содержания и логической структуры, конфиденциальности (закрытости для посторонних лиц), и выражается через шесть форм проявления уязвимости информации.

Прежде всего, угроза должна иметь какие-то сущностные проявления, а любое проявление принято классифицировать явлением, поэтому, одним из признаков и вместе с тем одной из составляющих угроз должно быть явление.

В основе любого явления лежат составляющие причины, которые являются его движущей силой и которые в свою очередь обусловлены некоторыми предпосылками или обстоятельствами.

Эти обстоятельства и причины относятся к факторам, создающим возможность дестабилизирующего воздействия на информацию.

Таким образом, факторы считаются её одним признаком и составляющей угрозы.

Ещё одним особым признаком угрозы считается её направленность, то есть итог, к которому может привести дестабилизирующее воздействие на информацию.

Угроза защищаемой информации – множество явлений, условий и факторов, создающих опасность нарушения статуса информации.

Для раскрытия структуры угроз нужно признаки угроз конкретизировать содержательной частью, которые в свою очередь обязаны раскрыть характер факторов и явлений, определить из состава и состав условий.

К сущностным проявлениям угрозы относятся:

1. виды дестабилизирующего воздействия на информацию (каким образом);
2. источник дестабилизирующего воздействия на информацию (от кого или чего исходят эти воздействия);
3. способы дестабилизирующего воздействия на информацию (какими приёмами, действиями осуществляются и реализуются виды дестабилизирующего воздействия).

К факторам кроме обстоятельств и причин нужно отнести наличие методов и каналов несанкционированного доступа к конфиденциальной информации для воздействия на информацию со стороны лиц, не имеющих к ней разрешённого доступа.

Анализ угроз информационной безопасности позволяет выделить составляющие современных компьютерных угроз - их источники и силы, которые движут, способы и последствия реализации. Анализ исключительно важен для получения всей необходимой информации об информационных угрозах, определения потенциальной величины ущерба, как материального, так и нематериального, и выработки адекватных мер противодействия.

При анализе угроз информационной безопасности используются три основных метода:

прямая экспертная оценка;

статистический анализ;

факторный анализ.

Рассмотрим приведенные методы подробнее:

Прямая экспертная оценка. Метод экспертных оценок основан на том, что параметры угроз задаются экспертами. Эксперты определяют перечни параметров, характеризующих угрозы информационной безопасности, и дают субъективные коэффициенты важности каждого параметра.

Статистический анализ - это анализ информационных угроз на основе накопленных данных об инцидентах информационной безопасности, в частности, о частоте возникновения угроз определенного типа, их источники и причины успеха или неуспеха реализации. Например, знание частоты появления угрозы позволяет определить вероятность ее возникновения за определенный промежуток времени. Для эффективного применения статистического метода необходимо наличие достаточно большого по объему базы данных об инцидентах. Нужно отметить еще одно требование: при использовании объемных баз необходимые инструменты обобщения данных и выявления в базе уже известной и новой информации.

Анализ основан на выявлении факторов, которые с определенной вероятностью ведут к реализации угроз и тех или иных негативных последствий.

Такими факторами могут быть наличие привлекательных для киберпреступников информационных активов, уязвимости, высокий уровень вирусной активности во внешней среде и т. д.

Поскольку современные информационные системы влияют множество факторов, обычно используется многофакторный анализ.

Как правило, системы управления состоят из следующих основных структурно-функциональных элементов:

рабочих станций - отдельных электронно-вычислительных машин (далее - ЭВМ) или терминалов сети, на которых реализуются автоматизированные рабочие места пользователей (абонентов, операторов) серверов (служб файлов, печати, баз данных и т.п.) не выделенных (или выделенных, то есть не совмещенных с рабочими станциями) высокопроизводительных ЭВМ, предназначенных для реализации функций хранения, печати данных, обслуживание рабочих станций сети и т. п. действий;

сетевых устройств (маршрутизаторов, коммутаторов, шлюзов, центров коммутации пакетов, коммуникационных ЭВМ) - элементов, обеспечивающих соединение нескольких сетей передачи данных, или нескольких сегментов одной и той же сети, возможно, имеют различные протоколы взаимодействия;

каналов связи (локальных, телефонных, с узлами коммутации и т. д.).

Рабочие станции являются наиболее доступными компонентами сетей и именно из них могут быть приняты наиболее многочисленные попытки совершения несанкционированных действий.

С рабочих станций осуществляется управление процессами обработки информации, запуск программ, ввода и корректировки данных, на дисках рабочих станций могут размещаться важные данные и программы обработки. На мониторы и печатая устройства рабочих станций, выводится информация при работе пользователей (операторов), выполняющих различные функции и имеют различные полномочия по доступу к данным и других ресурсов системы. Именно на рабочих станциях осуществляется ввод имен и паролей пользователями.

Поэтому рабочие станции должны быть надежно защищены от доступа посторонних лиц и содержать средства разграничения доступа к ресурсам со стороны задекларированных пользователей, имеющих различные полномочия.

Кроме того, средства защиты должны предотвращать нарушения нормальной настройки (конфигурации) рабочих станций и режимов их функционирования, вызванные непреднамеренным вмешательством неопытных (невнимательных) пользователей особой защите нуждаются такие привлекательные для злоумышленников элементы сетей как серверы и сетевые устройства.

Первые - как концентраторы больших объемов информации, вторые - как элементы, в которых осуществляется преобразование (возможно через открытую, незашифрованную форму представления) данных при согласовании протоколов обмена в различных участках сети.

Благоприятной для повышения безопасности серверов и сетевых устройств обстоятельством является наличие возможностей их надежной защиты физическими средствами и организационными мерами в силу их выделения, позволяет сократить до минимума число лиц из персонала, которые имеют непосредственный доступ к ним. Иными словами, непосредственные случайные воздействия персонала и умышленные локальные действия злоумышленников на выделенные серверы и сетевые устройства можно считать маловероятными. Но, все более распространенными становятся массированные атаки на серверы и сетевые устройства (а также и на рабочие станции) с использованием средств удаленного доступа. Здесь злоумышленники, прежде всего, могут искать возможности повлиять на работу различных подсистем рабочих станций, серверов и сетевых устройств, используя недостатки протоколов обмена данными и средств разграничения удаленного доступа к ресурсам и системных таблиц. Использоваться могут все возможности и средства, от стандартных (без модификации компонентов) до подключения специальных аппаратных средств (каналы, как правило, слабо защищены от подключения) и применения специализированных программ для преодоления системы защиты. Приведенное выше не значат, что не будет попыток внедрения аппаратных и программных закладок в самые сетевые устройства и серверы, которые открывают широкие дополнительные возможности по несанкционированному удаленного доступа. Закладки могут быть внедрены как с удаленных станций (с помощью вирусов или иным способом), так и непосредственно в аппаратуру и программы серверов при их ремонте, обслуживании, модернизации, переход на новые версии программного обеспечения, изменении оборудования.

Каналы и средства связи также нуждаются в защите. В силу большой пространственной протяженности линий связи (через неконтролируемую или слабо контролируемую территорию) практически всегда существует возможность

подключения к ним, или вмешательства в процесс передачи данных которые открывают широкие дополнительные возможности по несанкционированному удаленного доступа. Закладки могут быть внедрены как с удаленных станций (с помощью вирусов или иным способом), так и непосредственно в аппаратуру и программы серверов при их ремонте, обслуживании, модернизации, переход на новые версии программного обеспечения, изменении оборудования.

ЗАКЛЮЧЕНИЕ

Таким образом, информационная безопасность (information security) - сохранение конфиденциальности, целостности и доступности информации; кроме того, могут учитываться другие свойства, такие, как аутентичность, прослеживаемость, неопровержимость и надежность.

Информационная безопасность - состояние защищенности жизненно важных интересов человека, общества и государства, при котором предотвращается нанесение ущерба через: неполноту, несвоевременности и недостоверность информации, используемой; негативное информационное влияние; негативные последствия применения информационных технологий; несанкционированное распространение, использование и нарушение целостности, конфиденциальности и доступности информации.

Информационная безопасность - это комплексная многоуровневая система, которая охватывает интересы человека, общества, государства, еще следовало бы добавить международного сообщества.

Проблемы защиты от информации существенно сложнее проблемы защиты информации, поскольку угрозы от информации чрезвычайно разнообразные, их влияние не всегда очевиден, он осуществляется намеренно, изящно и коварно, а предотвращения этих угроз и нейтрализация требуют различных неординарных действий. Информационные угрозы является сложным иерархическим образованием с множеством разноуровневых связей, их влияние на человека комплексно и разнообразно.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Гафнер, В. В. Информационная безопасность / В.В. Гафнер. - М.: Феникс, 2017. - 336 с.

2. Гришина, Н. В. Информационная безопасность предприятия. Учебное пособие / Н.В. Гришина. - М.: Форум, 2015. - 240 с.
3. Информационная безопасность открытых систем. В 2 томах. Том 1. Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников и др. - Москва: Машиностроение, 2016. - 536 с.
4. Информационная безопасность открытых систем. В 2 томах. Том 2. Средства защиты в сетях / С.В. Запечников и др. - Москва: Наука, 2017. - 560 с.
5. Информационная безопасность систем организационного управления. Теоретические основы. В 2 томах. Том 1. - М.: Наука, 2016. - 496 с.
6. Мельников, В. П. Информационная безопасность и защита информации / В.П. Мельников, С.А. Клейменов, А.М. Петраков. - Москва: Машиностроение, 2014. - 336 с.
7. Партыка, Т. Л. Информационная безопасность / Т.Л. Партыка, И.И. Попов. - М.: Форум, Инфра-М, 2012. - 368 с.
8. Партыка, Т.Л. Информационная безопасность / Т.Л. Партыка, И.И. Попов. - М.: ИНФРА-М, 2012. - 368 с.
9. Сальная, Л. К. Английский язык для специалистов в области информационной безопасности / Л.К. Сальная, А.К. Шилов, Ю.А. Королева. - М.: Гелиос АРВ, 2016. - 208 с.
10. Степанов, Е.А. Информационная безопасность и защита информации. Учебное пособие / Е.А. Степанов, И.К. Корнеев. - М.: ИНФРА-М, 2017. - 304 с.
11. Федоров, А. В. Информационная безопасность в мировом политическом процессе / А.В. Федоров. - М.: МГИМО-Университет, 2016. - 220 с.
12. INFOBEZ-EXPO — международная выставка-конференция [Электронный ресурс]. — 2013. — Режим доступа: \www/ URL: http://infobez-expo.ru/
13. Информационная безопасность бизнеса [Электронный ре сурс]. — 2012. — Режим доступа: \www/URL: http://www. kaspersky.ru/other/custom-html/brfwn/Bezopasnost_Screen.pdf
14. Аверченков, В. И. Формализация процесса выбора состава средств обеспечения безопасности на объекте защиты [Текст] / В. И. Аверченков, М. Ю. Рытов, Т. Р. Гайнулин // Вестник компьютерных и информационных технологий. — 2010. — № 11. — С. 45–50.
15. Сулавко, А. Е. Технологии защиты от внутренних угроз информационной безопасности [Текст] / А. Е. Сулавко // Вестник СибАД. — 2011. — № 1(19) — С. 45–51.
16. Инсайдерские угрозы в России 2009 [Электронный ре сурс]. — 2009. — Режим доступа: \www/URL: http://www. perimetrix.ru/downloads/rp/PTX_Insider_Security_Threats_ in_Russia_2009.pdf

17. Коржов, В. В. Защита персональных данных: проблемы и пути решения [Текст] / В. В. Коржов // Открытые си стемы. — 2010. — № 10. — С. 11.
18. Марков, А. П. Проблемы и решения по защите персональ ных данных в информационных системах персональных данных [Текст] / А. П. Марков, Б. И. Сухинин // Компью терная безопасность. — 2009. — № 5. — С. 20–27.