Содержание:

Введение

В современном мире информационные технологии охватывают все сферы человеческой жизни, формируя информационное единство всей человеческой цивилизации. Через глобальную сеть Интернет объединяются и передаются на любые расстояния гигантские объемы информации. Множество пользователей, проживающих на территории всей планеты получают доступ информационным ресурсам всего мирового сообщества. По данным Росстата в Российской Федерации количество компьютеров только в организациях за 2003-2017 годы увеличилось на 8,6154 млн. единиц, а доступ в интернет за этот период получили 7,5879 млн. (приложение 1).

На сегодняшний день вопросы информационной безопасности не могут оставаться без соответствующего внимания, иначе последствия могут быть катастрофическими как для отдельных лиц, так и для общества в целом. Искажение, фальсификация, уничтожение или разглашение информации, нарушение процессов ее обработки и передачи наносят серьезный материальный и моральный ущерб многим людям, организациям и государству, чьи интересы заключаются в том, чтобы определенный объем информации, касающаяся их экономических, политических и других сфер деятельности, конфиденциальной информации был бы легко доступен авторизованному пользователю и вместе с тем огражден от возможных рисков. Для этой проблемы существует такой вид деятельности как информационная безопасность.

Целью данной работы является определение вида и состава угроз информационной безопасности во множестве их проявлений.

1 Понятие и структура угроз защищаемой информации

Информационная безопасность - защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб

субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры. Защита информации– это комплекс мер, направленных на обеспечение информационной безопасности. Таким образом методологически правильный подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов.

Все многообразие интересов субъектов, касающихся взаимодействия с информационными системами, можно разделить на следующие категории: обеспечение доступности, целостности и конфиденциальности информационных ресурсов и поддерживающей инфраструктуры. Доступность – это возможность за приемлемое время получить требуемую информационную услугу. Исходя из этого правила, доступ к информации должен предоставляться авторизованным лицам тогда, когда им это необходимо. Основными факторами, способными повлиять на доступность информационных систем, являются DDoS-атаки (Distributed Denial of Service — «отказ в обслуживании»), атаки программ-вымогателей (Ransomware), саботаж. Кроме того, источником угроз доступности являются непреднамеренные человеческие ошибки, совершенные по оплошности или ввиду недостаточной профессиональной подготовки: случайное удаление файлов, записей в базах данных, неверные настройки систем; выход из строя по причине превышения предельно допустимой мощности или недостаточности ресурсов оборудования, аварий сетей связи; неудачное обновление аппаратного или программного обеспечения; отключение систем из-за аварий энергоснабжения. Достаточно значительную роль в нарушении доступности могут исполнять такие природные катастрофы как землетрясения, ураганы, пожары, наводнения и аналогичные им явления. Тем не менее в каждом из описанных вариантов конечный пользователь утрачивает доступ к информации, которая необходима для осуществления его деятельности, и вынужден дожидаться окончания ликвидации последствий. Ценность системы для отдельного пользователя и её значение для существования самой организации определяют уровень влияния времени простоя. Неудовлетворительные меры безопасности увеличивают вероятность поражения вредоносными программами, уничтожения или повреждения данных, вторжения извне или DDoS-атак. Такого рода происшествия способны сделать системы недоступными для обычных пользователей

Целостность - актуальность и непротиворечивость информации, ее защищенность от несанкционированных изменений, повреждений или разрушения. Безошибочное выполнение операций или принятие правильных решений в организации

осуществимо лишь на основе достоверных данных, хранящихся в файлах, базах данных или системах, или распространяемых через компьютерные сети. Иначе говоря, информация должна быть защищена от преднамеренного, несанкционированного или случайного изменения, а также от возможных искажений в процессе хранения, транзакции или обработки. Угрозу ее целостности могут представлять компьютерные вирусы, логические бомбы, ошибки программирования, вредоносные изменения программного кода, подмена данных, не авторизованный доступ, черви, бэкдоры и т.п. Кроме направленных действий, зачастую несанкционированные изменения важной информации происходят из-за технических сбоев или человеческих ошибок по неосторожности или как результат недостаточной профессиональной подготовки. Так например, к нарушению целостности могут приводить: случайное удаление файлов, ввод неправильных значений, изменение настроек, выполнение неверных команд, как рядовыми пользователями, так и системными администраторами.

Для защиты целостности информации необходимо применение множества разнообразных мер контроля и управления изменениями информации и обрабатывающих её систем. Таким примером является ограничение круга лиц с правами на изменения лишь теми, кому такой доступ необходим для выполнения своих должностных обязанностей. При этом следует соблюдать принцип разграничения полномочий, согласно которому изменения в данные или информационную систему вносит одно лицо, а подтверждает их или отклоняет - другое. Кроме того, любые изменения должны быть согласованны и протестированы на предмет обеспечения информационной целостности и внесены в систему только корректно сформированными транзакциями. Обновления программного обеспечения необходимо производить с соблюдением мер безопасности. Любые действия способные повлечь нежелательные изменения, должны быть обязательно протоколированы.

Конфиденциальность– это защита от несанкционированного доступа к информации. Конфиденциальность информации достигается предоставлением к ней доступа с наименьшими привилегиями исходя из принципа минимальной необходимой осведомленности. Другими словами, авторизованное лицо должно иметь доступ только информации необходимой для исполнения его должностных обязанностей. Упомянутые выше преступления против неприкосновенности частной жизни, такие, как кража личности, являются нарушениями конфиденциальности. Одной из важнейших мер обеспечения конфиденциальности является классификация информации, позволяющая относить её

конфиденциальной, предназначенной для публичного или внутреннего пользования.

Информационные системы создаются для получения определенных информационных услуг. Если по каким-либо причинам предоставление этих услуги пользователям представляется невозможным — это наносит ущерб всем сторонам информационных отношений. В результате, доступность, не противореча остальным аспектам, выделяется как важнейший элемент информационной безопасности.

Целостность можно подразделить на:

-статическую, определяемую как неизменность информационных объектов;

-динамическую, относящуюся к безошибочному выполнению сложных действий. Средства контроля динамической целостности применяются, в частности, при анализе потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений.

Угроза — потенциально возможное событие, вызваемое действием, процессом или явлением, которое воздействуя на информацию, ее носители и процессы обработки способно привести к ущемлению интересов определенных субъектов.

Нарушение безопасности — реализация угрозы безопасности (наступление соответствующего события).

Различают два вида угроз безопасности:

-
  - несанкционированное распространение сведений — утечка информации (разглашение, разведка, несанкционированный доступ к информации);
  - несанкционированное воздействие на информацию и ее носители — воздействие на информацию с нарушением установленных прав и правил на изменение информации. Несанкционированное действие бывает целенаправленным (искажение, уничтожение, копирование, блокирование утрата, сбой функционирования носителя информации) и непреднамеренным (ошибки пользователей и персонала, сбои и отказы техники, природные явления и другие случайные воздействия).

Разглашение информации — действие, в результате которого доступ к информации получает неконтролируемое числу лиц.

Разведка — целенаправленная деятельность по получению сведений в интересах информационного обеспечения военно-политического руководства другого государства или конкурирующей организации.

Существуют агентурный и технический виды разведки. Агентурная разведка ведется оперативниками (сотрудники оперативного подразделения государственного органа или негосударственной структуры) с привлечением агентов (лица, конфиденциально сотрудничающие с разведывательной структурой) и специалистов (лица, обладающие специальными знаниями, умениями и навыками, привлекаемые в целях оказания помощи в сборе, исследовании, оценке и использовании информации).

Под технической разведкой понимается целенаправленная деятельность по добыванию с помощью технических систем, средств и аппаратуры сведений в интересах информационного обеспечения военно-политического руководства другого государства или конкурирующей организации, подготовки и ведения информационной борьбы. Источником данной угрозы является деятельность иностранных разведывательных и специальных служб, иностранных общественных организаций (в том числе коммерческих), а также деятельность отечественных преступных группировок и отдельных лиц.

Основные отличия разведки от разглашения заключаются в том, что информация, добытая с помощью разведки, становится доступна ограниченному кругу лиц. Разведка, как правило, ведется с враждебными целями, тогда как разглашение может таких целей и не преследовать. Разведка всегда ведется умышленно, а разглашение нередко является результатом неосторожности обладателя информации.

Под несанкционированным доступом к информации следует понимать действие, результатом которого является нарушение правил разграничения доступа, и получение информации лицом, не имеющим соответствующего права. Следствием несанкционированного доступа не всегда становится утечка информации, несанкционированный доступ может совершаться в целях активного воздействия на информацию, получения незаконных привилегий, удовлетворения амбиций и т.п. Несанкционированный доступ может являться результатом как умышленных, так и неумышленных (ошибки в организации защиты информации, недостаточная

квалификация персонала и т.д.) действий. Элементы несанкционированного доступа присутствуют и при ведении разведки, и при несанкционированном воздействии на информацию. Тем не менее, разведка (например, путем сбора открытых сведений) и несанкционированные воздействия могут осуществляться без несанкционированного доступа к информации или ее носителю.

Несанкционированное воздействие на информацию и ее носитель можно классифицировать следующим образом:

- Модификация информации – осуществляется, как правило, без предварительного ознакомления, иначе будет иметь место утечка. Возможна модификация как следующий шаг после организации утечки. Различают следующие виды модификации информации:
  - Уничтожение – наблюдается при хакерском проникновении в вычислительные системы, при стихийных бедствиях и т.д.;
  - Искажение – если злоумышленник получил доступ к каналу передачи информации, но не может ознакомиться с самой информацией, например вследствие ее зашифрованности, то он может попытаться внести в нее ложные данные в целях нанесения ущерба владельцу. Искажение может возникать непреднамеренно как следствие помех в канале передачи;
  - Подделка – широко используется при фальсификации банковских операций, осуществляемых в электронном виде;
- Блокирование доступа к информации – встречается в том случае, когда злоумышленник не может сам воспользоваться информацией, но имеет доступ к средствам ее обработки и своими действиями препятствует законному владельцу обрабатывать эту информацию;
- Хищение носителя;
- Утрата носителя.

1.1 Классификация угроз безопасности

Основными источниками угроз информации являются:

- стихийные бедствия (наводнение, ураган, землетрясение, пожар и т.д.);
- аварии, сбои и отказы оборудования;
- ошибки проектирования и разработки компонентов (автоматизированных систем, аппаратных средств, технологии обработки информации, программ, структур данных и т.д.);

- ошибки эксплуатации (пользователей, операторов и другого персонала);
- преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов и т.д.).

Источники угроз могут быть как внешними, так и внутренними (например, аппаратура, персонал, программы, конечные пользователи).

На сегодняшний день перечень угроз информационной безопасности содержит сотни позиций, вкупе с оценкой вероятности их реализации и моделью нарушителя он служит основой для анализа риска реализации угроз и формулирования требований к системе защиты. Помимо выявления вероятных угроз разумно также проведение анализа этих угроз на основе их классификации по некоторым признакам. Каждый из этих признаков олицетворяет одно из универсализированных требований к системе защиты.

Классификация угроз информационной безопасности необходима вследствие того, что хранимая и обрабатываемая информация подвластна воздействию крайне большого числа факторов, из-за чего становится невозможно формализация описания всего спектра угроз. Следствием этого стала необходимость определять для защищаемой системе не весь перечень угроз, а перечень классов угроз.

Классификацию вероятных угроз можно провести по таким определяющим признакам.

- По источнику возникновения:
  - Естественные угрозы, обусловленные объективными физическими процессами или стихийными природными явлениями;
  - Искусственные угрозы, являющиеся следствием действий человека.
- По степени преднамеренности:
  - Непреднамеренные угрозы, являющиеся следствием ошибок или халатности персонала;
  - Преднамеренные угрозы, вызванные целенаправленными действиями злоумышленников.
- По непосредственному источнику угроз:
  - Природная среда (например, стихийные бедствия);
  - Человек (шпионаж, разглашение или порча информации и т.д.);
  - Санкционированные программно-аппаратные средства (удаление данных, отказ в работе);

    - Несанкционированные программно-аппаратные средства (например, вирусы и прочие вредоносные программы).
- По расположению источника угроз:
    - Вне контролируемой зоны (перехват данных или побочных электромагнитных, акустических и прочих излучений);
    - В пределах контролируемой зоны (кража распечаток, записей или носителей информации);
    - В самой системе (например, некорректное использование ресурсов).
- По степени зависимости от активности системы:
    - Независимые от активности (вскрытие шифров криптозащиты);
    - Зависимые от активности системы (распространение вирусов и выполнение их кода).
- По степени воздействия:
    - Пассивные угрозы, не изменяющие структуру и содержание системы (копирование данных);
    - Активные угрозы, при воздействии вносящие изменения данные или нарушающие работоспособность системы.
- По этапам доступа к ресурсам:
    - Проявляющиеся на этапе доступа к ресурсам (несанкционированный доступ);
    - Проявляющиеся после получения доступа к ресурсам (несанкционированное или некорректное использование ресурсов системы).
- По способу доступа к ресурсам:
    - Реализуемые с использованием стандартного пути доступа к ресурсам (кража паролей и других атрибутов разграничения доступа с дальнейшей маскировкой под зарегистрированного пользователя);
    - Реализуемые с использованием нестандартного пути доступа к ресурсам (несанкционированный доступ методом использования недокументированных возможностей системы).
- По месту размещения информации, хранимой и обрабатываемой в системе:
    - Угрозы доступа к информации на внешних носителях (копирование информации с винчестера);
    - Угрозы доступа к информации, расположенной в оперативной памяти (чтение остаточной информации, доступ к системной области оперативной памяти);

    - Угрозы доступа к информации передаваемой по линиям связи (незаконное подключение к линиям связи и последующие манипуляции с передаваемыми данными);
    - Угрозы доступа к информации, отображаемой на дисплее или распечатанной на принтере.

Потенциальные угрозы по источнику своего возникновения подразделяют на естественные и искусственные.

Естественные угрозы – вызваны воздействиями объективных физических процессов или стихийных природных явлений, которые не зависят от действий человека; искусственные угрозы – связаны непосредственно с деятельностью людей.

Выделяют непреднамеренные (случайные, неумышленные) и преднамеренные (умышленные) искусственные угрозы.

Непреднамеренные искусственные угрозы могут возникать из-за ошибок в проектировании автоматизированных систем и их элементов, ошибок в программном обеспечении, в действиях персонала и т.д.

К основным вариантам непреднамеренных искусственных угроз (действиям, совершаемым людьми случайно – по незнанию, невнимательности или халатности) относят:

- частичный или полный отказ системы или разрушение аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление или искажение файлов с важной информацией или программ и т.д.);
- произвольное отключение оборудования или изменение режимов работы устройств и программ;
- непреднамеренная порча носителей информации;
- запуск технологических программ, которые при неграмотном использовании могут вызвать потерю работоспособности или необратимые изменения в системе (форматирование или переразметку носителей информации, удаление данных и т.д.);
- нелегальная инсталляция и использование непредусмотренных программ (игровых, обучающих, технологических и пр.), не являющихся необходимыми для выполнения пользователем своих служебных обязанностей и последующее необоснованное расходование ресурсов (загрузка процессора,

захват оперативной памяти и памяти на внешних носителях);
- заражение компьютера вирусами;
- неосторожные действия, приводящие к разглашению конфиденциальной информации;
- разглашение, передача или утеря реквизитов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
- проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, представляющих опасность для работоспособности системы и информации;
- пренебрежение установленными правилами при работе в системе;
- вход в систему в обход средств защиты (загрузка посторонней операционной системы со сменных носителей и т.п.);
- некомпетентное использование, настройка или произвольное отключение средств защиты персоналом службы безопасности;
- пересылка данных по неверному адресу;
- ввод ошибочных данных;
- непреднамеренное повреждение каналов связи.

Преднамеренные искусственные угрозы обусловлены корыстными, идейными или иными намерениями людей (злоумышленников).

Возможны следующие методы умышленного нарушения работы, вывода системы из строя, проникновения в систему и несанкционированного доступа к информации:

- физическое разрушение системы (взрыв, поджог и т.п.) или вывод из строя отдельных, жизненно необходимых компонентов системы (устройств, носителей системной информации и т.д.);
- отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.д.);
- нарушение функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т.п.);
- внедрение агентов в число персонала (в том числе в административную группу, отвечающую за безопасность);
- вербовка (путем подкупа или шантажа) персонала или отдельных пользователей, имеющих определённые полномочия;

- применение подслушивающих устройств, дистанционных фото- и видеосъемки и пр.;
- перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания, системы пожарно-охранной сигнализации, видеонаблюдения и т.д.) и инженерные коммуникации (системы отопления, кондиционирования, заземления и т.п.);
- перехват данных, передаваемых по каналам связи, и их анализ в целях выяснения протоколов обмена, правил вхождения в сеть и авторизации пользователей и последующих попыток их имитации для проникновения в систему;
- кража носителей информации (дисков, флэш-карт);
- несанкционированное копирование носителей информации;
- кража производственных отходов (распечаток, записей);
- чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств или из областей оперативной памяти операционной системой в асинхронном режиме, используя недостатки мультизадачных операционных систем и систем программирования;
- нелегальное получение паролей и иных атрибутов разграничения доступа (агентурным путем, подбором пароля, имитацией интерфейса системы, используя халатность пользователя и т.д.) с последующей выдачей себя за зарегистрированного пользователя;
- несанкционированное использование пользовательских терминалов, имеющих уникальные физические идентификаторы, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т.д.;
- взлом шифров криптозащиты информации;
- внедрение аппаратных «спецвложений», программных закладок и вирусов (например, «трояны), то есть таких участков программ, которые позволяют преодолевать систему защиты, осуществлять доступ к системным ресурсам с целью регистрации и передачи критичной информации или нарушения функционирования системы;
- незаконное подключение к линиям связи для работы с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений, или в целях прямой подмены законного пользователя путем его физического отключения

после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений .

Следует отметить то, что самым распространенным, вариативным и опасным источником угрозы воздействия на защищаемую информацию является непосредственно человек, так как воздействие на защищаемую информацию могут оказывать самые разные категории людей, как работающие на предприятии, так и не являющиеся его сотрудниками.

1.2 Угрозы информационной безопасности в сети Интернет

Сегодня практически любой человек имеет в своем распоряжении компьютер в каком-либо проявлении (Стационарный ПК, ноутбук, планшет, смартфон) и имеет доступ к глобальной сети Интернет, и потому с высокой долей вероятности может столкнуться с теми или иными угрозами информационной безопасности на «бытовом уровне». Виды угроз, с которыми может столкнуться рядовой пользователь можно выделить в отдельный список в связи с некоторой их спецификой.

В зависимости от различных способов классификации угрозы информационной безопасности, связанные с сетью Интернет для рядового пользователя, можно разделить на следующие основные подгруппы:

-нежелательный контент

-несанкционированный доступ

-утечки информации

-потеря данных

-мошенничество

Нежелательный контент представляет собой не только вредоносные, потенциально опасные программы и спам, непосредственно созданные для уничтожения или кражи информации, но и сайты, запрещенные законодательством, или нежелательные сайты, содержащие информацию, не соответствующую возрасту потребителя.

Несанкционированный доступ — просмотр информации лицом, не имеющим права пользоваться данной информацией. Несанкционированный доступ приводит к утечке информации. В зависимости от типа информации и способа ее хранения, утечки могут осуществляться разными способами, такими как атаки на сайты, взлом программ, перехват данных по сети, использование несанкционированных программ.

Утечка информации в зависимости от того, чем она была вызвана, может быть на умышленной и случайной. Случайные утечки происходят из-за ошибок оборудования, программного обеспечения и человека. А умышленные организовываются преднамеренно, с целью получить доступ к данным либо нанести ущерб. Потерю данных можно выделить как одну из основных угроз информационной безопасности. Нарушение целостности информации может быть вызвано неисправностью оборудования, умышленными действиями пользователей или по неосторожности.

Не менее опасной угрозой является фрод (мошенничество с использованием информационных технологий). К мошенничеству можно отнести не только манипуляции с кредитными картами и взлом онлайн-банка, но и внутренний фрод (мошеннические действия, совершаемые персоналом с использованием своего положения и доступа к оборудованию) . Целью этих экономических преступлений является обход законодательства, политики, нормативных актов компаний, присвоение имущества. Количество мошеннических схем, применяемых злоумышленниками в сети Интернет, постоянно растет и для неопытного пользователя, пожалуй, именно они представляют наибольшую угрозу.

1.3 Источники угроз информационной безопасности в среде Интернет

Нарушение информационной безопасности может быть вызвано как целенаправленными действиями злоумышленника, так и неопытностью пользователя. Пользователь должен иметь хоть какое-то базовое представление об информационной безопасности, вредоносном программном обеспечении, возможных мошеннических схемах, чтобы своими действиями не нанести ущерб самому себе или компании, в которой он работает.

Чтобы пробиться через защиту и получить доступ к нужной информации злоумышленники используют уязвимости и ошибки в работе программного обеспечения, web-приложений, ошибки в конфигурациях файрволлов, прав доступа, прибегают к прослушиванию каналов связи и использованию клавиатурных шпионов. Пользуясь неопытностью пользователя, злоумышленник может получить нужную информацию выдавая себя, например, за работника банка, технической поддержки, оператора связи и т.д.

Потеря информации может быть обусловлена не только внешними атаками злоумышленников и неаккуратностью пользователей, но и работниками компании, которые заинтересованы в получении прибыли в обмен на ценные данные организации, в которой работают или работали. Источниками угроз выступают отдельные лица или группы, специализирующиеся на преступной деятельности в цифровом пространстве и государственные спецслужбы (киберподразделения), которые используют весь арсенал доступных кибесредств. То, каким образом будет производиться атака, зависит от типа информации и ее расположения, способов доступа к ней и уровня защиты.

Подходить к оценке угроз 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 напряжение, проводить резервное копирование информации, что актуально в большей мере для организаций, чем для бытового применения. Следует устанавливать и регулярно обновлять программное обеспечение. Отдельное внимание нужно уделять защитному программному обеспечению, базы которого должны обновляться ежедневно.

Обучение пользователей основам информационной безопасности и принципам работы различных вредоносных программ поможет избежать случайных утечек данных, а также исключить случайную установку потенциально опасных программ на компьютер. Для слежения за деятельностью сотрудников компаний на рабочих местах и обнаружения злоумышленника следует использовать DLP-системы.

Организовать информационную безопасность помогут специализированные программы, разработанные на основе современных технологий. Примером таких технологий предотвращения утечек конфиденциальной информации являются DLP-системы. А в борьбе с мошенничеством следует использовать анти-фрод системы,

которые предоставляют возможность отслеживать, обнаруживать и управлять уровнем фрода.

Отсутствие достаточных навыков и опыта работы с вычислительной техникой и глобальной сетью, а также недостаточная осведомленность в вопросах обеспечения личной информационной безопасности является наиболее распространенным источником угрозы безопасности. Знание простейших правил безопасности (что можно, а что не стоит делать при работе в сети, посещения каких веб-сайтов лучше избегать, осторожность при работе с почтой и т.п.) и понимание того, к каким последствиям может привести нарушение этих правил поможет избежать массы неприятностей с которыми зачастую сталкиваются люди, не имеющие достаточного опыта и знаний, при работе в сети.

2 Информационная безопасность государства

Государство — это организация политической власти, охватывающая определенную территорию и выступающее одновременно как средство обеспечения интересов всего общества и как особый механизм управления обществом на основе права. «Информационное наполнение» деятельности государства определяется деятельностью его органов по стимулированию развития информационной инфраструктуры и активной информационной деятельности граждан по защите их прав и свобод в этой области, а также по обеспечению законных ограничений на ознакомление с информацией ограниченного доступа, несанкционированное раскрытие или использование которой может нанести ущерб интересам личности, общества и государства. Нанесение вреда деятельности органов государства способно существенно снизить их возможности по выполнению государственных функций. Например, безнаказанное нарушение тайны переговоров, личной и семейной тайны подрывает доверие граждан к государству, уменьшает социальную поддержку государственной политики; подделка таможенных деклараций лишает его возможности поддерживать устойчивое функционирование экономической сферы общества.

Информационная безопасность государства заключается в защищенности от угроз его способности получать, обрабатывать, хранить, передавать и распространять информацию, необходимую для управления обществом, выполнения законодательной, правоприменительной, правоохранительной и судебной

функций, а так же сохранять определенную часть информации в тайне от других лиц.

Угрозы информационной безопасности государства могут проявляться в процессе взаимодействия прежде всего с другими государствами или с некоторыми социальными группами общества (например, организованным преступным сообществом). Проявление угроз, как правило, ослабляет возможности данных органов по выполнению возложенных функций и тем самым ущемляет интересы государства.

В настоящее время наиболее опасными угрозами информационной безопасности государств мира признаются угрозы преднамеренного использования информационно-коммуникационных технологий государствами для достижения военно-политических целей, для подготовки и осуществления терактов, а также угрозы дальнейшего увеличения социальной опасности компьютерной преступности.

Несмотря на то, что «холодная война" давно завершена, в настоящее время проблема информационной безопасности стоит еще более остро, поскольку значительно возросла роль накопления, обработки и распространения информации, в частности, в принятии стратегических решений, увеличилось количество субъектов информационных отношений и потребителей информации. Информация играет все большую роль в процессе жизнедеятельности человека. Об этом свидетельствует хотя бы тот факт, что средства массовой информации часто называют "четвертой" властью (наряду с законодательной, исполнительной и судебной).

Часто самые опасные информационные воздействия называют информационным оружием. Информационное оружие - это средства уничтожения или хищения информационных массивов, получения из них необходимой информации после проникновения через системы защиты, ограничения или запрета на доступ к ним законных пользователей, нарушение работы технических средств, вывода из строя телекоммуникационных сетей, компьютерных систем, различных средств высокотехнологического обеспечения жизни общества и функционирования государства.

Информационная безопасность предполагает не только защиту от информационного оружия, но и обеспечение конституционных прав граждан на свободу сбора, распространения и получения информации (естественно, с

определенными ограничениями), на тайну корреспонденции и т.п. Это и многое другое должно быть урегулировано законодательством о коммерческой, служебной и профессиональной тайне, об информации персонального характера и др.

Организационной основой создания и развития системы информационной безопасности, существующей в рамках национальной системы безопасности, являются:

- ○ ▪ Стратегия развития информационного общества Российской Федерации от 07.02.2008 года № Пр-212;
  ▪ Доктрина информационной безопасности Российской Федерации от 05.12.2016 года № 646;
  ▪ Федеральные законы и нормативные акты;
  ▪ Концептуальные, программные и иные документы.

Государственная политика определяет основные направления концептуального развития и практических действий научно-технического, информационного, экономического и социального характера в сфере информационной безопасности.

Основу системы государственного регулирования составляет совокупность:

- ○ ▪ Федеральных органов исполнительной власти;
  ▪ Органов исполнительной власти субъектов Российской Федерации;
  ▪ Органов местного самоуправления;
  ▪ Основных объектов регулирования деятельности (организации, учреждения, специализированные предприятия, структурные подразделения по информационной безопасности, системы, комплексы, защищаемые объекты и т.д.).

В организационном плане функционирование системы и регулирование деятельности осуществляется на основных принципах, в том числе:

- ○ ▪ Обеспечение национальных интересов государства;
  ▪ Оптимальное сочетание правовых, организационных, технических мер;
  ▪ Своевременное выявление видов и направленности угроз и их нейтрализация;
  ▪ Приоритетность направлений по предотвращению ущерба;

- Адекватность и дифференцированность, системность и комплексность реализации мер по информационной безопасности.

В соответствии с федеральными законами от 28.12.2010 г. №390-ФЗ «О безопасности» и 28.06.2014 г. №172-ФЗ «О стратегическом планировании в Российской Федерации» указом президента от 31.12.2015 г. №683 «О стратегии национальной безопасности Российской федерации» была утверждена новая Стратегия национальной безопасности Российской федерации, пришедшая на замену предыдущей. Стратегия национальной безопасности Российской Федерации, являющаяся базовым документом стратегического планирования, устанавливает национальные интересы и стратегические национальные приоритеты Российской Федерации, уточняет политику государства в сфере обеспечения национальной безопасности на долгосрочную перспективу. Реализация Стратегии национальной безопасности Российской Федерации в качестве информационной основы включает в себя федеральную информационную систему стратегического планирования и строится на организации информационной безопасности с учетом стратегических национальных приоритетов.

Основополагающим нормативным актом о государственной политике и развитии общественных отношений в области обеспечения информационной безопасности, выработке способов по совершенствованию системы обеспечения информационной безопасности является утвержденная указом Президентом Российской Федерации от 5 декабря 2016 года №646 «Доктрина информационной безопасности Российской Федерации».

В данной Доктрине на основании анализа основных информационных угроз и оценки состояния информационной безопасности определены стратегические цели и основные направления обеспечения информационной безопасности с учетом стратегических национальных приоритетов Российской Федерации.

Все чаще возможности сети Интернет используются для достижения различных военно-политических и террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности.

На сегодняшний день Интернет является инструментом с самыми различными вариантами его применения, в том числе и в целях нанесения ущерба, причем не только отдельным гражданам, но и целым государствам. Упреждающим шагом на

законодательном уровне в нашей стране было принятие Федерального закона от 26.07.2017 г. № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации", вступивший в силу с 2018 года.

В развитие его положений в начале 2018 года по предложению Минкомсвязи России функции технического центра (оператора реестров) национальных доменов RU/РФ было передано в структуры "Ростелеком", вновь созданному ООО "Технический центр Интернет".

01.05.2019 был принят федеральный закон №90-ФЗ (так называемый «Закон о суверенном Рунете»), согласно которому были внесены изменения в федеральные законы «О связи» и «Об информации». Этот закон вызвал множество отрицательных отзывов от пользователей и крайне неоднозначное отношение к нему экспертов, согласно которым данный закон принесет больше вреда чем пользы и направлен в первую очередь на цензурирование информации, а не на обеспечение реальной безопасности (по мнению некоторых экспертов, реализация данного законопроекта сделает российский сегмент Интернета даже более уязвимым).

Таким образом информационная безопасность государства зачастую зависит от людей плохо разбирающихся в данной теме, преследующих свои политические интересы и не всегда прислушивающихся к мнению специалистов, что может приводить к принятию решений в частности вызывающих снижение уровня информационной безопасности государства или ущемление прав граждан прописанных в Доктрине и Конституции Российской Федерации.

2.1 Виды угроз информационной безопасности Российской Федерации

Согласно Доктрине информационной безопасности Российской Федерации, угрозы информационной безопасности подразделяются на следующие категории:

- угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;
- угрозы информационному обеспечению государственной политики Российской Федерации;

- угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;
- угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Угрозами конституционным правам и свободам человека в сфере духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию могут являться:

- принятие федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации нормативных правовых актов, ущемляющих конституционные права и свободы граждан в области духовной жизни и информационной деятельности;
- создание монополий на формирование, получение и распространение информации в Российской Федерации, в том числе с использованием телекоммуникационных систем;
- противодействие, в том числе со стороны криминальных структур, реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;
- нерациональное, чрезмерное ограничение доступа к общественно необходимой информации;
- противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание;
- неисполнение федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, организациями и гражданами требований федерального законодательства, регулирующего отношения в информационной сфере;
- неправомерное ограничение доступа граждан к открытым информационным ресурсам федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, к открытым архивным материалам, к другой открытой социально значимой информации;
- дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы;

- нарушение конституционных прав и свобод человека и гражданина в области массовой информации;
- вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур;
- девальвация духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям, принятым в российском обществе;
- снижение духовного, нравственного и творческого потенциала населения России, что существенно осложнит подготовку трудовых ресурсов для внедрения и использования новейших технологий, в том числе информационных;
- манипулирование информацией (дезинформация, сокрытие или искажение информации).

Угрозами информационному обеспечению государственной политики Российской Федерации могут являться:

- монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами;
- блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории;
- низкая эффективность информационного обеспечения государственной политики Российской Федерации вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики.

Угрозами развитию отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов могут являться:

- противодействие доступу Российской Федерации к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов, а также создание условий для усиления

технологической зависимости России в области современных информационных технологий;
- закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам;
- вытеснение с отечественного рынка российских производителей средств информатизации, телекоммуникации и связи;
- увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности.

Угрозами безопасности информационных и телекоммуникационных средств и систем, как существующих, так и создаваемых на территории Российской Федерации, могут являться:

- противоправные сбор и использование информации;
- нарушения технологии обработки информации;
- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
- уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;
- воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;
- компрометация ключей и средств криптографической защиты информации;
- утечка информации по техническим каналам;
- внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;
- уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;
- перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;
- использование не сертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств

информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;
- несанкционированный доступ к информации, находящейся в банках и базах данных;
- нарушение законных ограничений на распространение информации.

2.2 Источники угроз информационной безопасности Российской Федерации

Источники угроз информационной безопасности Российской Федерации, в зависимости от характера проявления вредоносного воздействия подразделяются на внешние и внутренние.

К внешним источникам относятся:

- деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, ориентированных на подрыв интересов Российской Федерации в информационной сфере;
- тяга ряда стран к господству и ущемлению интересов России в мировом информационном пространстве, вытеснению ее со всех информационных рынков;
- обострение международной конкуренции за право владения информационными технологиями и ресурсами;
- нарастающая с каждым годом деятельность международных террористических организаций;
- увеличение технологического преимущества ведущих держав мира и увеличение их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;
- деятельность космических, воздушных, морских и наземных технических и иных средств разведки иностранных государств;
- разработка некоторыми государствами концепций информационных войн, которые предусматривают создание средств вредоносного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

К внутренним источникам относятся:

- критическое состояние отечественных отраслей промышленности;
- неблагоприятная криминогенная обстановка, которую сопровождают тенденции сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, наращивание влияния организованной преступности на жизнь общества, понижение уровня защищенности законных интересов граждан, общества и государства в информационной сфере;
- неудовлетворительная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Российской Федерации;
- недостаточная проработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;
- неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;
- недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;
- недостаточная экономическая мощь государства;
- снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;
- недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;
- отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

2.3 Информационная война

Непосредственной угрозой информационной безопасности Российской Федерации в настоящее время является информационная война.

Информационная война (information warfare) – всестороннее воздействие, оказываемое во время кризиса или конфликта на определенного противника для решения установленных задач.

Термин «информационная война» занимает особое место в исследованиях современных проблем информационной безопасности. Впервые он был введен в употребление в Соединенных Штатах советником по науке Министерства обороны Томасом Роном в докладе «Системы оружия и информационной войны», подготовленном для компании «Боинг» в 1976 году, в котором отмечалось, что информационная инфраструктура становится ключевым компонентом экономики США и в то же время является уязвимой целью в военное и мирное время. Официально он появился в директиве министра обороны США «Информационная война» ("Information Warfare") от 21 декабря 1992 года. Соответственно, Соединенные Штаты впервые в мире официально сформулировали основы стратегии информационного противостояния сразу после завершения войны в Персидском заливе 1991 года, где американские вооруженные силы первыми применили в том числе новейшие информационные технологии. В августе 1995 году Национальный университет обороны США опубликовал статью «Что такое информационная война?» одного из крупнейших американских ученых в информационной области, специалиста корпорации RAND профессора Мартина Либицки, разработавшего одну из первых классификаций составляющих информационной войны XXI века и рассмотрел ее как состоящую из семи различных элементов:

-Война в области контроля и управления ведется на реальном поле боя. Она направлена на каналы связи между командованием и исполнителями. Пресекая эти каналы, нападающая сторона стремится добиться нарушения работы систем управления войсками, линий связи и систем управления противника в целом на стратегическом, оперативном или тактическом уровнях. Следовательно, атакующая сторона изолирует командование от исполнителей.

-Разведывательная война – сбор важной в военном отношении информации и защита собственной – благодаря развитию информационных технологий, позволяет

получить дополнительные данные о противнике.

-Электронная война предполагает действия против средств электронных коммуникаций: радиосвязи, радаров, компьютерных сетей и т.д. Ее важным элементом является криптография.

-Психологическая война – использование информационных возможностей и ресурсов против человеческого сознания (существуют четыре формы ее ведения: культурный конфликт, подрыв национальной идеи, военного руководства или войск противника). В качестве важного средства ее ведения М. Либицки рассматривает средства массовой информации.

-Основным средством поражения в «хакерской» войне являются компьютерные вредоносные программы (в том числе вирусы), целью которых являются компьютерные сети. Их нарушение может происходить как в мирное, так и военное время, как в отношении военных, так и государственных и частных компьютерных систем и информационных ресурсов. С военной точки зрения в зависимости от целей и объектов операции могут быть оборонительными и наступательными.

-Экономическая информационная война направлена на коммерческую информацию и может принимать одну из двух основных форм –информационная блокада и информационный империализм. Она основана на предположении, что в будущем государства будут зависеть от информационных потоков так же, как на сегодняшний день они зависят от материального обеспечения и обмена.

-Кибервойна направлена на дестабилизацию компьютерных систем и доступа к Интернет государственных учреждений, финансовых и деловых центров, а также на создание беспорядка и хаоса в жизни стран и государств, полагающихся на интернет в своей повседневной жизни.

Заключение

В связи с ростом числа устройств имеющих доступ в Интернет, увеличением числа организаций, предприятий большого, среднего и малого бизнеса использующих автоматизированные системы и глобальные сети для ведения бизнеса, общей компьютеризации жизни общества, ростом числа компьютерных преступлений и случаев промышленного шпионажа, увеличением напряженности в

международных отношениях информационная безопасность с каждым годом становится все более важной сферой деятельности.

Угрозой информации – является сочетание различных условий и факторов, определяющих возможную или действительно существующую опасность, сопряженную с утечкой, повреждением или уничтожением информации, несанкционированными или непреднамеренными воздействиями на нее. Реальными угрозами можно считать такие, осуществление которых способно нанести вред государству, организации или частному лицу и которые могут быть реализованы на объекте информатизации. Самым опасным и многогранным источником угрозы для информации на любом уровне (на уровне государства, организаций или же бытовом) является человек, так как на защищаемую информацию могут оказывать воздействие самые разнообразные категории людей или их группы, имеющие совершенно разные цели и возможности.

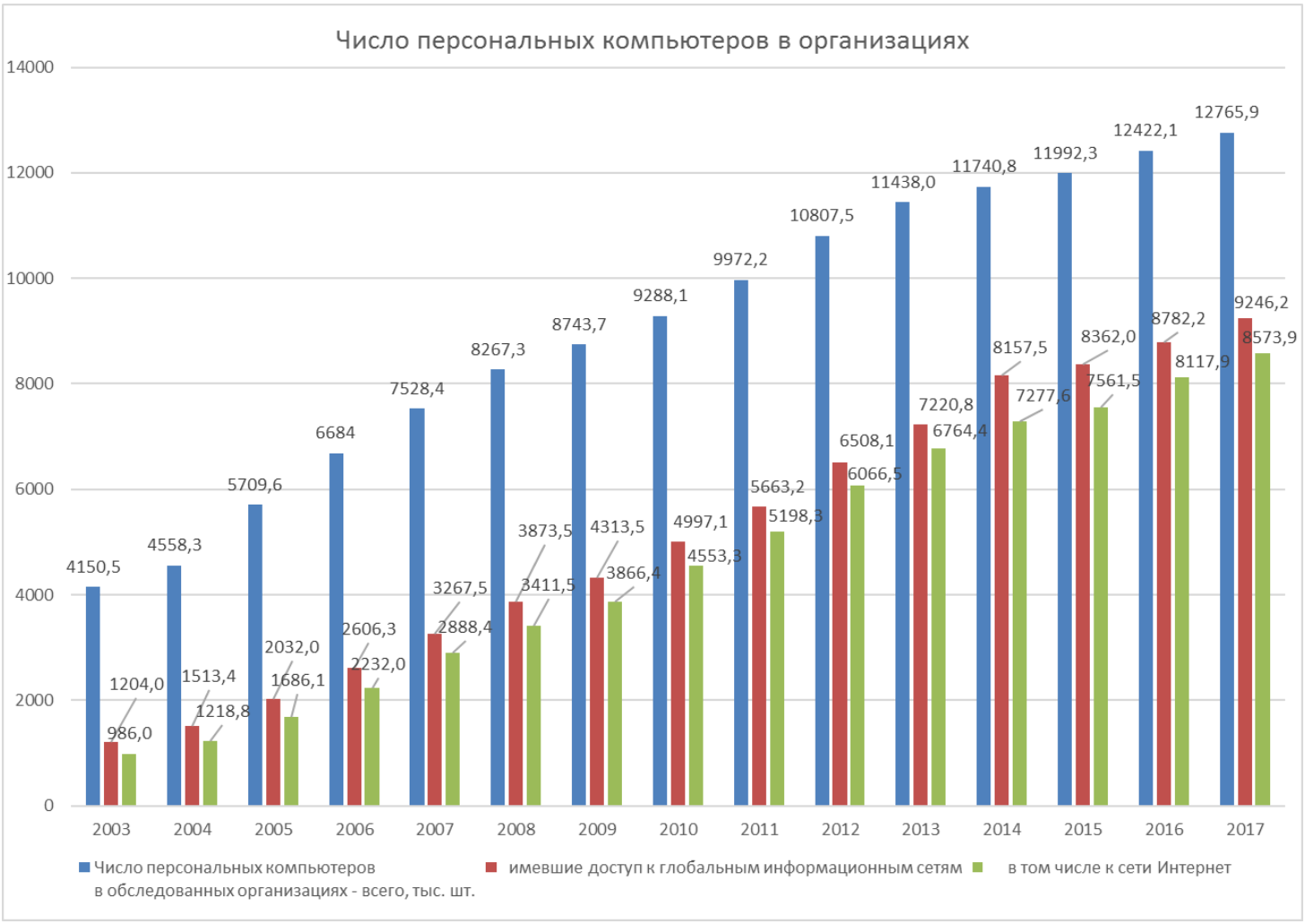
Все многообразие видов и способов вредоносного воздействия на защищаемую информацию приводит к необходимости комплексной системы защиты информации, заключающемся в сочетании различных организационных (организация службы безопасности, программ обучения и повышения квалификации персонала и пр.) и программно-технических мер и средств с учетом требований нормативной и технической документации.

Государственная политика Российской Федерации в сфере информационной безопасности проводится с учетом развития в стране информационного общества и совершенствования системы государственного управления, базирующегося на использовании информационных и телекоммуникационных технологий. Положения, отраженные в новой доктрине, действительно актуальны, так как описывают текущее состояние информационной безопасности в Российской Федерации и отмечают проблемы и информационные угрозы, направленные на все сферы деятельности общества.

Список литературы

1. Гатчин Ю. А., Сухостат В. В., Куракин А. С., Донецкая Ю. В. Теория информационной безопасности и методология защиты информации – 2-еизд., испр. И доп. – СПб: Университет ИТМО, 2018. – 100 с.

2. В. В. Бондарев, Введение в информационную безопасность автоматизированных систем: учебное пособие -Москва: Издательство МГГУ им. Н. Э. Баумана, 2016. -250 с.
3. А.В. Загорскоий, Н.П. Ромашкина Угрозы информационной безопасности в кризисах и конфликтах XXI века –. –М.: ИМЭМО РАН, 2015. –151 с.
4. Шабуров А. С. Информационная безопасность предприятия: Учебно-методическое пособие. – Перм. нац. исслед. политехн. ун-т. – Пермь, 2011., 68 с.
5. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. — М.: ИД «ФОРУМ»: ИНФРА-М, 2011. — 416 с.
6. А. А. Стрельцов Организационно-правовое обеспечение информационной безопасности: учебник/ под редакцией А. А. Александрова, М. П. Сычева. – Москва: Издательство МГТУ им. Н. Э. Баумана, 2018. – 291 с.
7. www.gks.ru.
8. Доктрина информационной безопасности Российской Федерации от 5 декабря 2016 года №646.
9. www.anti-malware.ru



Приложение 1