Содержание:

Введение

Информация, как ресурс, несет в себе значительную ценность, поэтому при нынешней информатизации общества очень важно сохранить целостность и неприкосновенность передаваемой информации.

Под информационной безопасностью понимается 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.

Угрозы информационной безопасности – это оборотная сторона использования информационных технологий. Выборочная и бессистемная реализация мероприятий, направленных на повышение уровня IT-безопасности, не сможет обеспечить необходимого уровня защиты.

Актуальность и важность проблемы обеспечения информационной безопасности обусловлена многочисленными факторами:

-быстрые темпы роста парка персональных компьютеров, применяемых в разнообразных сферах человеческой деятельности из-за увеличения обрабатываемой информации;

-резкое расширение сферы пользователей, имеющих непосредственный доступ к вычислительным ресурсам и массивам данных;

-доступность корпоративной информации через мобильные устройства (ноутбук, КПК, смартфон).

-доступность средств персональных ЭВМ, привела к распространению компьютерной грамотности в широких слоях населения.

-значительное увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью компьютеров и других средств автоматизации.

-стремительное развитие информационных технологий, открыло новые возможности эффективной работы предприятия, однако привело и к появлению новых угроз.

Анализ угроз информационной безопасности позволяет определить, какие мероприятия эффективны для их минимизации и предотвращения, а какие нет.

Целью данной курсовой работы является изучение теоретических основ информационной безопасности, а также рассмотрение видов и состава угроз информационной безопасности.

Для решения поставленной цели, были выдвинуты следующие задачи:

1) описать понятие информационной безопасности;

2) рассмотреть основные составляющие информационной безопасности;

3) описать виды угроз информационной безопасности;

4) проанализировать источники угроз информационной безопасности;

5)описать особенности деятельности фонда региональных социальных программ;

6) проанализировать защиту информации в Фонде региональных социальных программ.

Объектом исследования данной курсовой работы является информационная безопасность.

Предмет работы - угрозы информационной безопасности.

Основу исследования составляют метод системного анализа, статистический и метод правового анализа.

Данная курсовая работа состоит из введения, двух глав, заключения, списка литературы.

Глава 1. Теоретические основы определения информационной безопасности

1.1 Понятие информационной безопасности и ее составляющие

До недавнего времени национальная безопасность рассматривалась как сохранение суверенитета и территориальной целостности государства, его устойчивость перед угрозой применения вооруженной силы со стороны других государств. Однако, в настоящее время, национальная безопасность видится как комплексная системная проблема, учитывающая наличие многообразных факторов и угроз, в том числе информационных. Таким образом, национальная безопасность Российской Федерации зависит от обеспечения информационной безопасности, и, в ходе развития технического прогресса, быстрыми темпами растущего использования современных информационных технологий, эта зависимость неизбежно возрастает. Значимость информационной безопасности для Российской Федерации обусловлена тем, что информационная сфера обеспечивает функционирование всех остальных сфер жизни общества и государства.

Основным документом, определяющим политику нашей страны в сфере информационной безопасности, является Доктрина информационной безопасности Российской Федерации, утвержденная Президентом РФ 05 декабря 2016 г. № 646. В этом документе информационная безопасность Российской Федерации понимается, как состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

Информационная безопасность достигается не только за счет средств, методов и мероприятий, направленных на защиту информационной среды и защиту объекта (субъекта) от деструктивного воздействия, но и посредством развития способности у объекта (субъекта) уклоняться от деструктивного информационного воздействия. Задача обеспечения информационной безопасности состоит в том, чтобы создать оптимальные условия для функционирования информационной инфраструктуры, главный элемент которой не компьютер, а человек мог прогрессивно развиваться и действовать сообразно своим ценностям и целям.

При исследовании понятия и сущности информационной безопасности нельзя не помянуть о безопасности самой информации. В целях обеспечения

информационной безопасности органы исполнительной власти обязаны выполнять требования о защите информации, содержащейся в государственных информационных системах, которые устанавливаются уполномоченными федеральными органами исполнительной власти.

Безопасность информации, как составляющая информационной безопасности, включает в себя защиту информации и информационных ресурсов от несанкционированного доступа, искажения, уничтожения, установление режима информации в зависимости от ее содержания, обеспечение защиты сведений, составляющих государственную тайну, иной информации ограниченного доступа. Детальное регламентирование данных правоотношений содержится в Законе Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне».

Безопасность информации обеспечивается различными мерами: организационными, техническими, правовыми. Согласно ст. 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» указанные меры по защите информации направлены:

– на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

– соблюдение конфиденциальности информации ограниченного доступа;

– реализацию права на доступ к информации.

Перечисленные меры представляют собой установление в отношении конкретных видов информации правового режима и обеспечение его соблюдения. Их исполнение возложено на обладателя информации, оператора информационной системы в случаях, установленных законодательством Российской Федерации.

Применительно к информации, циркулирующей в сфере государственного управления, обладателями информации, операторами государственных информационных систем по общему правилу являются органы исполнительной власти. Ограничения в доступе к информации, находящейся у органов исполнительной власти, устанавливаются в том случае, когда иные меры регулирования не могут обеспечить должный правовой порядок, в первую очередь безопасность. Это достигается при помощи следующих средств:

– установление дополнительных запретов и обязываний, ограничение определенных действий;

– принятие специальных мер, направленных на установление и поддержание режимных правил;

– разрешительный способ и тип реализации прав и свобод;

– система контроля и надзора за выполнением режимных требований;

– установление ответственности за нарушение специального правового режима.

В целях обеспечения информационной безопасности Российской Федерации предусмотрено создание государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных а так на информационные ресурсы Российской Федерации – информационные системы и информационно-телекоммуникационные сети, находящиеся на территории Российской Федерации и в дипломатических представительствах и консульских учреждениях Российской Федерации за рубежом.

Основными задачами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации установлены:

а) прогнозирование ситуации в области обеспечения информационной безопасности Российской Федерации;

б) обеспечение взаимодействия владельцев информационных ресурсов Российской Федерации, операторов связи, иных субъектов, осуществляющих лицензируемую деятельность в области защиты информации, при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак;

в) осуществление контроля степени защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак;

г) установление причин компьютерных инцидентов, связанных с функционированием информационных ресурсов Российской Федерации.

Одним из последних документов, посвященных информационной безопасности, является Указ Президента РФ от 22 мая 2015 г. № 260 «О некоторых вопросах информационной безопасности Российской Федерации». Согласно ему, сегмент

международной компьютерной сети Интернет для федеральных органов государственной власти и органов государственной власти субъектов РФ, находящийся в ведении Федеральной службы охраны РФ, должен быть преобразован в российский государственный сегмент информационно-телекоммуникационной сети Интернет. Отмечается, что подключение российских государственных органов к Интернету должно происходить по защищенным каналам связи с использованием шифровальных средств.

Исследование понятия информационной безопасности Российской Федерации позволило сформулировать следующие выводы:

1) Основное содержание понятия «информационная безопасность» заключается в обеспечении безопасности информации; защите субъектов, владеющих информацией, от негативного воздействия.

2) Безопасность информации, как составляющая информационной безопасности, включает в себя защиту информации и информационных ресурсов от несанкционированного доступа, искажения, уничтожения, установление режима информации в зависимости от ее содержания, обеспечение защиты сведений, составляющих государственную тайну, иной информации ограниченного доступа.

Как уже было отмечено ранее, информационная безопасность - многогранная область деятельности, в которой успех может принести только систематический, комплексный подход.

Обеспечение информационной безопасности в большинстве случаев связано с комплексным решением трех задач, обеспечивающих:

1) доступность информации;

2) целостность информации;

3) конфиденциальность информации.

Именно доступность, целостность и конфиденциальность являются равнозначными составляющими информационной безопасности.

1.Доступность информации

Информационные системы создаются для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги

пользователям невозможно, то это, очевидно, наносит ущерб всем пользователям.

Фактор времени в определении доступности информации в ряде случаев является очень важным, поскольку некоторые виды информации и информационных услуг имеют смысл только в определенный промежуток времени. Например, получение заранее заказанного билета на самолет после его вылета теряет всякий смысл. Точно так же получение прогноза погоды на вчерашний день не имеет никакого смысла, поскольку это событие уже наступило. В этом контексте весьма уместна поговорка: «Дорога ложка к обеду».

2. Целостность информации

Целостность информации условно подразделяется на статическую и динамическую. Статическая целостность информации предполагает неизменность информационных объектов от их исходного состояния, определяемого автором или источником информации. Динамическая целостность информации включает вопросы корректного выполнения сложных действий с информационными потоками, например, анализ потока сообщений для выявления некорректных, контроль правильности передачи сообщений, подтверждение отдельных сообщений.

Целостность является важнейшим аспектом информационной безопасности в тех случаях, когда информация используется для управления различными процессами, например, техническими, социальными.

3. Конфиденциальность информации

Конфиденциальность - самый проработанный у нас в стране аспект информационной безопасности. К сожалению, практическая реализация мер по обеспечению конфиденциальности современных информационных систем в России связана с серьезными трудностями. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишены возможности составить представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные и технические проблемы.

Нарушение каждой из трех рассмотренных категорий приводит к нарушению информационной безопасности в целом. Так, нарушение доступности приводит к отказу в доступе к информации, нарушение целостности - к фальсификации

информации и, наконец, нарушение конфиденциальности - к раскрытию информации. Базовые составляющие информационной безопасности приведены на рис. 1.

Рисунок 1- Базовые составляющие информационной безопасности

Как уже отмечалось, выделение этих категорий в качестве базовых составляющих информационной безопасности обусловлено необходимостью реализации комплексного подхода при обеспечении режима информационной безопасности. Кроме того, нарушение одной из этих категорий может привести к нарушению или полной бесполезности двух других. Например, хищение пароля для доступа к компьютеру (нарушение конфиденциальности) может привести к его блокировке, уничтожению данных (нарушение доступности информации) или фальсификации информации, содержащейся в памяти компьютера (нарушение целостности информации).

1.3 Виды угроз информационной безопасности

Угрозы информационной безопасности – это возможные действия или события, которые могут вести к нарушениям ИБ.

Виды угроз информационной безопасности очень разнообразны и имеют множество классификаций см.рис.2:

Виды угроз информационной безопасности

1.По характеру нарушения

-нарушение конфиденциальности данных.

-нарушение работоспособности ЭВМ.

-незаконное вмешательство в работу ЭВМ и прочее

-незначительные ошибки,-мелкое хулиганство

-серьезные преступления

2.По тяжести нарушения

-намеренные нарушения

-ненамеренные нарушения

3.По предвидению последствий нарушителем

4.По месту возникновения

нацеленные на всю ИС

нацеленные на отдельные компоненты ИС

5.По объекту воздействия

внешние или внутренние

-незначительные ошибки,-мелкое хулиганство

-серьезные преступления

6.По причине возникновения

7.По происхождению

-антропогенные

-техногенные

-природные

8.По каналу проникновения

-угрозы, проникающие через уязвимости ПО, съемные носители

-угрозы, проникающие через бреши в системах авторизации, недостатки систем хранения документов

Рисунок 2-Классификация угроз информационной безопасности

Угрозы информационного пространства - важная часть современной проблематики общества, которые в свою очередь делятся на две группы:

- Естественные угрозы могут возникнуть из-за стихийных событий и явлений, не зависящих от общества.

- Искусственные угрозы классифицируются на случайные и умышленные. Эта группа угроз напрямую обуславливаются обществом и происходят из-за беспечности, оплошностей и неопытности рабочих или специально соответственно.

Рассмотрев классификацию, угрозы можно поделить на семь ключевых структур:

1.Нежелательный контент.

2.Несанкционированный доступ.

3.Утечки информации.

4.Потеря данных.

5.Мошенничество.

6. Кибервойны.

7. Кибертерроризм.

Нежелательный контент – это опасные и вредящие приложения, рассылка, вебстраницы запрещенные законом и материалы не соответствующие возрастному ограничению.

Несанкционированный доступ – явление при котором работник не имеющий право обращаться к сокрытым данным, путем отступления от должностных возможностей, проникает к данным.

Утечка информации группируется на умышленную и случайную, последняя свершается из-за различных неполадок в техническом и программном оборудовании или недоработок сотрудников предприятия.

Потеря данных по праву считается важным аспектом угроз безопасности информационного пространства. Нарушение цельности информационных баз имеет вероятность быть спровоцировано неполадками оборудования или вредоносными событиями от пользователей, будь то они рабочими предприятия или вредителями.

Угрозу ИБ также представляет фрод (информационное мошенничество). К интернет - мошенничеству относят вредоносные операции с банковскими картами, взлом онлайн - банка, а также внутренний фрод.

Угрозы террористических организаций с каждым годом возрастают и появляются в виртуальном мире. Войны во всем мире меняют свой характер на информационные, в которых главным оружием является важная информация.

Нарушение информационной безопасности организации зависит от многих факторов, а также может быть запланированными действиями злоумышленника или же банальным отсутствия навыков у персонала. Не стоит забывать и про сотрудников, которые могут продавать информацию другим организациям, такой вариант дохода интересует их порой больше официального.

К оценке угрозам информационного пространства компании стоит подходить бережно, рассматривая множество факторов. Существует целый ряд защитных программных оболочек, базы которых необходимо обновлять ежедневно:

- защита от нежелательного контента (антивирус, антиспам, веб-фильтры, антишпионы), анти-ддос;

- фаерволы и системы обнаружения вторжений IPS;

- шифрование данных;

- резервное копирование;

- системы отказоустойчивости.

Невольные утечки данных и установку вредоносных программ можно избежать если в свое время обучать сотрудников организации основным навыкам работы в информационном пространстве.

В 21 веке мировую экономику потерпело значительные изменения, так появилась новые для социума «криптовалюты» и их способ заработка - криптомайнинг. Процесс заработка криптовалюты заключается в вычислительных операциях электронных машин, что также вызвало появление нелегальных способов заработка валют.

Компания «Trend Micro» сообщает, что к концу 2017 года в мире насчитывалось более 100 тысяч вредоносных программ для криптомайнинга.

Большую популярность набирает бестелесный криптомайнинг - способ внедрения в операционную систему различных вредоносных программ для криптойманинга. Обнаружить следы такой программы очень сложно, все что видит обычный пользователь - лишь исполняемый файл PoweShell и командный файл.

Заражение устройств путем установки вредоносных программ довольно распространенный способ, который дает доступ к вычислительной технике и ее ресурсам.

Предприятия все чаще прибегают к внедрению различных способов защиты, плагинов, фильтрации URL-адресов и прочих путей защиты от вредоносных программ.

Часто антивирусные программы и настройка шлюза сетевой безопасности обеспечивают защиту от несанкционированного криптомайнинга на самих устройствах.

В современном мире пользователь должен обладать рядом навыков и опытом владения электронными машинами. Конечно, обычная домохозяйка вряд ли противостоит атаки группы хакеров, но и такое событие встречается крайне редко. Зачастую пользователи попадают в неприятности из-за невнимательности и небрежности. Экономия на антивирусных программах, их отключение для получения доступа к другим ресурсам, установка программного обеспечения из сомнительных источников – все это имеет шанс заразить компьютер вирусами.

Домашние компьютеры рядовых пользователей являются привлекательной мишенью для киберпреступников, затратив малые усилия мошенники могут

раздобыть пароли доступа от банковских счетов и кредитных карт, украсть личные материалы для 189 последующего шантажа, а также устроить массовую хакерскую атаку используя зараженные компьютеры.

Одними из самых известных примеров вредоносных программ являются WannaCry и Petya, которые нанесли ущерб компаниям во всем мире и распространились на более чем 60 стран при этом нанеся в 8 млрд. долларов.

Анализируя современные тенденции развития информационных технологий и уровень организационных и технический мероприятий для обеспечения должного уровня информационной безопасности можно заметить актуальность проблем в нынешних условиях, когда массовые эпидемии компьютерных вирусов и информационные войны угрожают безопасности стран.

Ускоренное развитие информационных технологий в рамках перехода к цифровой экономике неизбежно приводит к своего рода соревнованию «снаряда и брони» - средств нападения и защиты в непрерывно идущей битве за обладание необходимой информацией, и мы должны сделать все зависящее от нас, чтобы не потерпеть поражение в этой битве. Как конкретно защитить себя и инфраструктуру компании от вредоносного майнинга и других угроз информационной безопасности – индивидуальный выбор, но пренебрегать угрозой не стоит, ведь в 21 веке информация имеет колоссальную ценность.

1.3 Источники угроз информационной безопасности

Причинами утечки информации могут быть различные события. Одной из основных угроз является сотрудник организации. Но его действия можно разделить на два случая: явные и неявные. В первом случае действует инсайдер исходя из своей выгоды. Во втором случае действия человека похожи на поведение инсайдера, но таковыми не являются, так как все его действия исходят от невнимательности или некомпетентности.

Безопасность информации организации напрямую зависит от защищенности технических каналов утечки конфиденциальной информации, которые подразумевают под собой неконтролируемый поток информативных сигналов.

Под каналами утечки информации понимают некую нежелательную цепочку носителей информации, среди которых имеются нарушители. Согласно другому определению под каналами утечки информации понимается путь, который информация может пройти от источника до получателя в процессе

несанкционированного доступа к ней.

Каналы утечки информации играют основную роль в защите информации, выступая фактором информационной безопасности.

Поскольку в природе существует всего четыре средства переноса информации, это световые лучи, электромагнитные и звуковые волны, материальные носители информации. Эти средства обязательно будут присутствовать в любой системе передачи информации.

А все каналы утечки информации можно разделить на четыре группы:

-материально-вещественные;

-аккустические;

-визуально-оптические;

-электромагнитные (они же ПЭМИН).

В качестве источника утечки информации может выступать сам человек, используя средство переноса информации из описанных выше.

Все каналы утечки данных можно разделить на косвенные и прямые. Косвенные каналы не нуждаются в доступе к техническим средствам информационной системы.

Прямые же наоборот, требуют доступа к аппаратному обеспечению и данным информационной системы.

Примеры косвенных каналов утечки:

- кража или потеря какого-либо носителя информации, не уничтоженный мусор может быть исследован на наличие информации;

- дистанционное фотографирование, прослушивание;

- перехват электромагнитных излучений.

Примеры прямых каналов утечки: [10]

- инсайдеры (человек внедренный конкурентами для получения информации). Утечка информации вследствие несоблюдения коммерческой тайны;

- прямое копирование.

Каналы утечки информации можно также разделить по физическим свойствам и принципам функционирования:

- акустические - запись звука, подслушивание и прослушивание;

- акустоэлектрические - получение информации через звуковые волны с дальнейшей передачей ее через сети электропитания;

- виброакустические - сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации защищаемых помещений;

- оптические - визуальные методы, фотографирование, видео съемка, наблюдение;

- электромагнитные - копирование полей путем снятия индуктивных наводок;

- радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств съема речевой информации «закладных устройств», модулированные информативным сигналом;

- материальные - информация на бумаге, диске, флеш-карте и прочих физических носителях информации.

Особенностью материально – вещественного канала утечки информации см.рис.1 являются его источники и носители информации, которыми являются люди и материальные объекты. Возможные причины утечки по материально – вещественному каналу:

1.Несовершенство политики безопасности организации.

2. Сбой в работе техники.

3.Утрата черновиков и чертежей.

4. Утерянные отходы делопроизводства.

Несанкционированный получатель информации

Источник информации

Носитель информации

Рисунок 3- Материальной - вещественный канал утечки

Прямой акустический сигнал см.рис.2 может распространяться в воде, воздухе и других гидромеханических средах. Для записи сигнала используют закладки со сверхчувствительными микрофонами, которые преобразуют акустический сигнал в электрический. Звукоизоляция будет хорошей профилактической мерой от утечки по данному каналу.

Источник фоновых колебаний

Усилитель

Вибродатчик

Объект воздействия

Среда распространения

Источник сигнала

Источник фоновых акустических шумов

Рисунок 4 - Акустический канал утечки информации [6]

Также существует виброакустический канал, который возникает по мере распространения звуковой волны в помещении, которая влияет на ограждающие конструкции встречающиеся на ее пути, вызывая в них колебания. Для перехвата такого типа информации используются средства акустической разведки: электронные стетоскопы и закладные устройства с датчиком контактного типа.

Побочные электромагнитные излучения (ПЭМИ) см рис.5 возникают в процессе протекания переменного электрического через технические средства обработки информации.

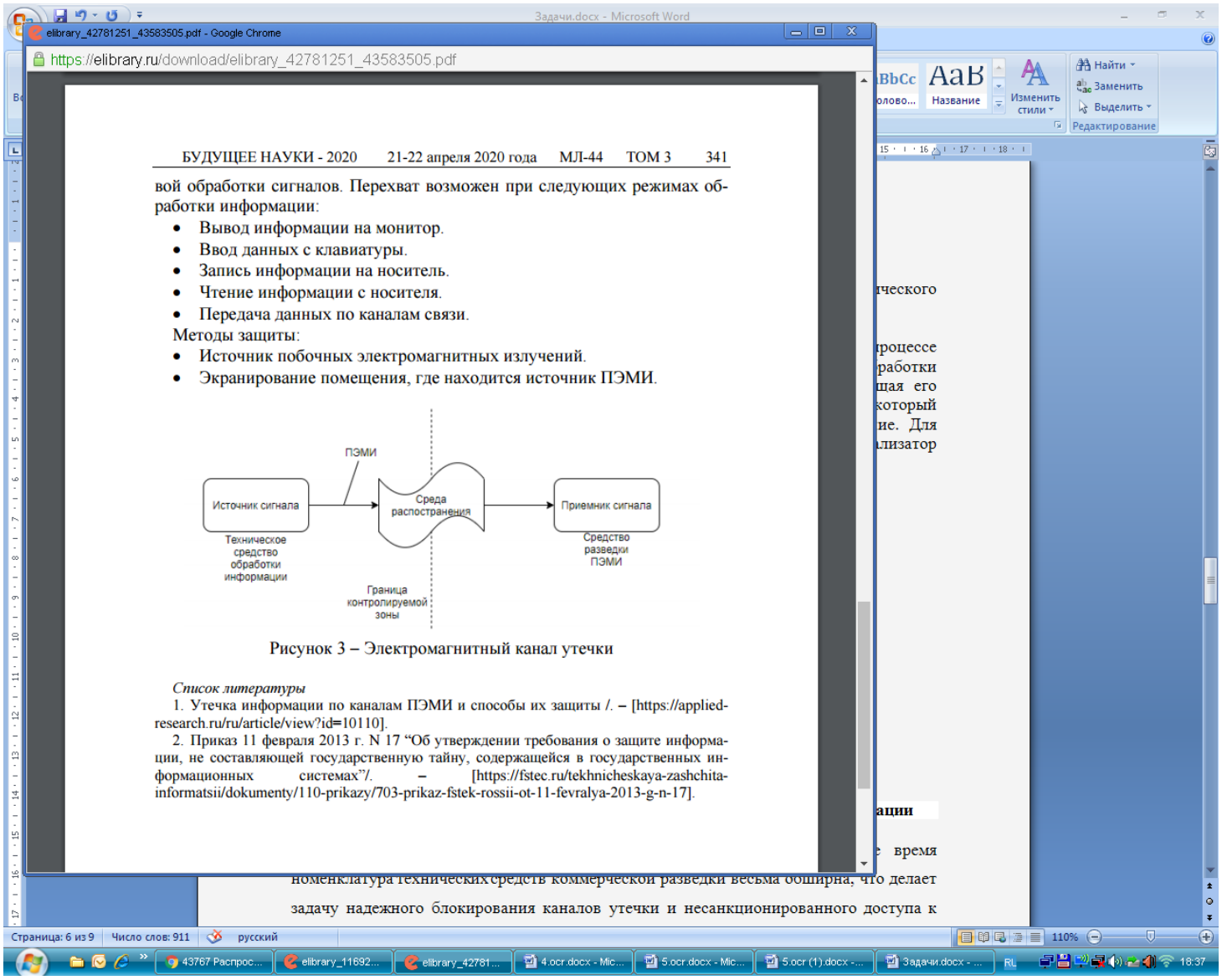

Рисунок 5- Электромагнитный канал утечки

Область, в которой возможен перехват ПЭМИ и последующая его дешифровка информации называется опасной зоной. Это зона, в пределах который соотношение, информативный сигнал/шум, превышают допустимое значение. Для перехвата ПЭМИ применяется следующие устройства: приемная антенна, анализатор спектра, устройств цифровой обработки сигналов.

Перехват возможен при следующих режимах обработки информации:

- Вывод информации на монитор.

- Ввод данных с клавиатуры.

- Запись информации на носитель.

- Чтение информации с носителя.

- Передача данных по каналам связи.

Итак, существует несколько способов классификации каналов утечки информации: прямые и косвенные каналы утечки информации или по физическим свойствам: акустические, акустоэлектрические, виброакустические, оптические, электромагнитные, радиоизлучения или электрические сигналы, материальные.

Глава 2. Анализ угроз информационной безопасности фонда региональных социальных программ «Наше будущее»

2.1 История создания и краткая характеристика Фонда

История создания Фонда относится к 2007 году. Тогда бизнесмен Вагит Алекперов генеральный директор Государственного нефтяного концерна «Лангепас УрайКогалымнефть» («Лукойл») принял соответствующее решение. Главная цель организации Фонда – это реализация долгосрочных социально значимых программ и проектов. В нашей стране это был первый частный фонд, ориентированный на принципы социального предпринимательства. Одной из главных задач фонда является помощь социально незащищенным слоям населения к которым относятся инвалиды, многодетные семьи, воспитанники детских домов и всем тем, кто в гражданской жизни часто остается невостребованным. Благодаря конкурсу идей, проводимым Фондом, социально незащищенные слои населения могут получить помощь в создании собственного бизнеса.

После создания Фонда первый всероссийский конкурс социальных проектов был проведен в 2008 году. По результатам конкурса был проведен отбор проектов для оказания адресной помощи. Первым лауреатом конкурса стала компания «Доспехи». Символично, что и деятельность самой компании направлена на оказание помощи: производство ортопедических систем для людей с повреждением спинного мозга.

Начиная с 2015 года фонд «Наше будущее» и МСП Банк поддерживают всероссийский конкурс проектов в области социального предпринимательства «Лучший социальный проект года», организованный Российским государственным социальным университетом совместно с Министерством экономического развития РФ.

Таким образом, к настоящему моменту фонд поддержал 254 проекта социального предпринимательства. Причем это не сводится только финансовой помощи, а включает и правовую, консультационную и информационную поддержку.

В 2020 году фонд занял 3 место в рейтинге Forbes среди лучших благотворительных фондов богатейших россиян.

За двенадцать лет существования фонда было выдано 254 беспроцентных займов для реализации проектов претендентов из 58 регионов нашей страны на общую сумму 653,2 миллиона рублей. Причем размер займа также постоянно увеличивается и на сегодня он составляет два миллиона рублей, а предприниматели, впервые участвующие в конкурсе, смогли претендовать на займы до 10 миллионов рублей, наравне с победителями прошлых лет. Фонд представляет достаточно комфортный срок погашения займа. Сегодня это 10 лет.

Фонд также взаимодействует с высшими учебными заведения России.

Таблица 1-Вузы, с которыми сотрудничает Фонд «Наше будущее»

№	Регион	Город	Организация	Год
1	Санкт-Петербург город	Санкт-Петербург город	Высшая школа менеджмента СПбГУ	2010
2	Москва	Москва	Российский государственный социальный университет	2014
3	Нижегородская область	Нижний Новгород	Нижегородский университет им. Н.И. Лобачевского	2014

4	Республика Татарстан	Казань	Казанский федеральный (Поволжский) университет	2015
5	Красноярский край	Красноярск	Сибирский федеральный университет	2015
6	Архангельская область	Архангельск	Северный (Арктический) федеральный университет	2015
7	Ставропольский край	Ставрополь	Северо-Кавказский федеральный университет	2015
8	Белгородская область	Белгород	Белгородский государственный национальный исследовательский университет	2015
9	Новосибирская область	Новосибирск	Новосибирский государственный университет экономики и управления	2015
10	Свердловская область	Екатеринбург	Уральский федеральный университет имени Б.Н.Ельцина	2015
11	Ростовская область	Ростов-на-Дону	Северо-Кавказский институт филиал РАНХиГС	2015
12	Республика Коми	Сыктывкар	Коми республиканская академия гос.службы и управления ГОУВО	2016
13	Москва	Москва	Российский экономический университет им. Г.В. Плеханова	2016

14	Москва	Москва	Институт Социального проектирования, НИИ ФГБОУ «РЭУ им. Г. В. Плеханова»	2016
15	Ростовская область	Ростов-на-Дону	Южный федеральный университет	2016
16	Пермский край	Пермь	Пермский государственный национальный исследовательский университет ВШЭ	2017
17	Иркутская область	Иркутск	Иркутский государственный университет	2017
18	Кировская область	Киров	Вятский государственный университет	2018
19	Республика Калмыкия	Элиста	Калмыцкий государственный университет	2018
20	Краснодарский край	Сочи	Сочинский государственный университет	2018
21	Волгоградская область	Волгоград	Волгоградский государственный университет	2019

Деятельность Фонда при сотрудничестве с ВУЗами направлена на разработку и внедрение курсов, связанных с предпринимательством для социально незащищенных групп. Благодаря деятельности Фонда в Сургуте была создана школа социального предпринимательства.

Еще одно из направлений деятельности Фонда – популяризация знаний. Для реализации этой цели Фонд активно работает с российским обществом «Знание».

2.2 Анализ защиты информации в Фонде региональных социальных программ

Организация Фонд «наше будущее» является оператором персональных данных. Это любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу, в том числе:

- его фамилия, имя, отчество,

- год, месяц, дата и место рождения,

- адрес, семейное, социальное, имущественное положение, образование, профессия, доходы,

- другая информация.

Персональные данные относятся к информации ограниченного доступа и должны защищаться в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных». Фонд зарегистрирован как оператор персональных данных в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Как оператор персональных данных в Фонде «Наше будущее» разработал ряд локальных нормативных документов, необходимых для обеспечения этойдеятельности:

1. Приказ «Об организации обработки персональных данных».
2. Приказ о назначении ответственного за организацию обработки персональных данных.
3. Согласие субъекта персональных данных на обработку его персональных данных.
4. Список лиц, допущенных к персональным данным, обрабатываемым в информационной системе.

На сайте Фонда представлена страница с политикой конфиденциальности.

В Фонде «Наше будущее» обрабатываются персональные данные трех категорий: сотрудники, клиенты и спонсоры.

Конфиденциальной информацией о сотрудниках Фонда «Наше будущее» является:

- дата, место рождения;

- адрес прописки или фактического жительства;
- семейное положение, состав семьи;
- биографические данные;
- сведения о доходах и имуществе;
- номера ИНН и СНИЛС; контакты – телефон, электронная почта;
- информация о воинской обязанности;
- медицинская информация и диагнозы.

Фотографии и видео с сотрудниками Фонда, а также имена и фамилии публикуются в открытом доступе на сайте организации и в отчетах о проделанной работе.

Конфиденциальной информацией о клиентах фонда является:

- фамилия, имя, отчество;
- дата, место рождения;
- адрес прописки или фактического жительства;
- семейное положение, состав семьи;
- биографические данные;
- профессиональная информация – образование, квалификация, должность, трудовой стаж, предыдущие места работы;
- сведения о доходах и имуществе;
- номера ИНН и СНИЛС; контакты – телефон, электронная почта;
- информация о воинской обязанности;
- медицинская информация и диагнозы.

Так как Фонд оказывает поддержку предпринимателям, в отчете Фонда и на его сайте, чаще всего, раскрывается информация о тех объектах социальной сферы, которые были модернизированы или построены за счет Фонда, но информация о тех лицах, которым Фонд выделил данные средства и которые осуществили перечисленные действия, не разглашается и является конфиденциальной информацией.

К конфиденциальной и охраняемой информации относится информация о спонсорах Фонда. В открытом доступе на сайте организации и в отчетах о работе отражаются подробно только средства, которые предоставлены Фонду государственным бюджетом, а сведения о частных спонсорах, их персональные и контактные данные являются строго конфиденциальной информацией.

Таким образом, система защиты конфиденциальной информации в Фонде связана с защитой коммерческой тайны и персональных данных.

В Фонде система защиты конфиденциальной информации ориентирована на:

- ограничение несанкционированного доступа (с целью модификации, изменения, уничтожения, копирования, распространения и прочих неправомерных действий):
- замки, двери, решетки на окнах, сигнализация и т.д. – любые средства, ограничивающие физический доступ к носителям информации;
- генераторы шума, сетевые фильтры и другие устройства, перекрывающие или обнаруживающие каналы утечки информации.
- разграничение доступа для сотрудников (персонала) Фонда;
- реализация прав доступа для работников Фонда.

Защита конфиденциальных данных в Фонде предполагает проработку таких решений для ИТ-инфраструктуры, которые позволяют:

- своевременного обнаружить факта несанкционированного доступа к информации;
- снизить уязвимость технических средств обработки и хранения информации;
- оперативно восстановить поврежденную, модифицированную информацию;
- предупредить о последствиях несанкционированного доступа к конфиденциальным данным.

Все средства и мероприятия в Фонде, нацеленные на защиту конфиденциальной информации, базируются на трех уровнях:

1. Правовой, обеспечивающий единый государственный стандарт по информационной защите, но не нарушающий права пользователей. Уровень регламентируется Законом РФ «Об информации, информационных технологиях и защите информации», подзаконными актами РФ, внутриорганизационными положениями о защите конфиденциальной информации, определяющими работу с «закрытой» документацией. На этом уровне в Фонде так выстроена информационная система и решения по ее защите, что они не нарушают права пользователей и нормы обработки данных.
2. Организационный, упорядочивающий работу с конфиденциальной документацией, определяющий степени и уровни доступа пользователей в информационные системы, носителями информации. Этот уровень

предотвращает утечку сведений по халатности или небрежности персонала Фонда, сводя его к минимуму.

Сюда относятся архитектурно-планировочные мероприятия и решения, структурирование систем запросов и выдача допусков на пользование Интернетом, корпоративной электронной почтой, сторонними ресурсами.

1. Права на получение и использование подписи в электронном цифровом виде, следование корпоративным и морально-этическим правилам, принятым внутри Фонда, также являются важными составляющими защиты конфиденциальных данных.

Технический уровень защиты конфиденциальной информации включает подуровни – аппаратный, криптографический, программный, физический.

Организационные мероприятия по защите конфиденциальной информации в Фонде выражаются в разработке регламента работы пользователей с информационной системой и информацией в ней. Правила доступа к системе были разработаны специалистами компании «Интергрус» совместно с руководством Фонда и службой безопасности.

Уровни правовой и организационной защиты данных являются неформальными средствами защиты информации. Кроме административных (организационных) регламентов и законодательных (правовых) норм сюда можно отнести и морально-этические правила.

В Фонде за счет комплекса административных и технических мероприятий осуществляется обеспечение защиты конфиденциальной информации на уровне организационной и правовой защиты:

- разграничение и реализация прав доступа к конфиденциальным сведениям;
- защита переговорных комнат, кабинетов руководства от прослушки;
- оформление службы запросов на доступ к информационным ресурсам (внутренним и внешним);
- получение и обучение работы с электронными цифровыми подписями (ЭЦП).

Техническая защита конфиденциальных сведений в Фонде осуществляется следующими средствами.

Физический, аппаратный, программный и криптографический уровни обеспечения защиты конфиденциальных данных относятся к формальным средствам.

Физический способ предполагает поддержание работы механизмов, являющихся препятствием для доступа к данным вне информационных каналов: замки, видеокамеры, датчики движения/излучения и т.п. Это оборудование действует независимо от информационных систем, но ограничивает доступ к носителям информации.

Аппаратными средствами безопасности считаются все приборы, монтируемые в телекоммуникационных или информационных системах Фонда: спецкомпьютеры, серверы и сети Фонда, система контроля работников, шумовые генераторы, любое оборудование, перекрывающее возможные каналы утечек и обнаруживающее «дыры» и т.д.

Программные средства представляет комплексное решение, предназначенное для обеспечения безопасной работы (системы, блокирующие возможную утечку данных и анализирующие реальные сигналы тревоги от устройств и приложений сетевого характера).

В Фонде «Наше будущее» для предотвращения утечек информации используется система SIEM (Security Information and Event Management, управление событиями и информационной безопасностью) – анализ в режиме реального времени сигналов об угрозах, ведение журнала данных, создание отчетов. SIEM представлены приложениями, приборами, программным обеспечением.

Криптографическая (математическая) защита позволяет безопасно обмениваться данными в глобальной либо корпоративной сетях Фонда. Математические преобразованные, шифрованные каналы считаются оптимально защищенными. Однако, стопроцентной защиты никто гарантировать, конечно, не может.

Криптография (шифрование) данных считается одним из самых надежных способов – технология сохраняет саму информацию, а не только доступ к ней. Средства шифрования обеспечивают защиту физических и виртуальных носителей информации, файлов и каталогов (папок), целых серверов Фонда.

Средства криптографической защиты конфиденциальной информации в Фонде обеспечивается за счет применения:

- криптопровайдеров (программных компонентов шифрования);
- организацией VPN;
- применением средств формирования, контроля и использования ЭЦП.

Техническая защита конфиденциальной информации в Фонде также реализуется через проведение аттестации – набора организационных и иных мероприятий, достаточных для безопасной работы с конфиденциальными данными. Аттестация базируется на требованиях и рекомендациях ФСТЭК, применяется для защищаемых помещений и автоматизированных систем.

Отсутствие или недостаточное внимание к одной из составляющих защиты конфиденциальной информации в Фонде может закончиться тем, что внутренние данные окажутся достоянием мошенников.

Заключение

Основное содержание понятия «информационная безопасность» заключается в обеспечении безопасности информации; защите субъектов, владеющих информацией, от негативного воздействия.

Безопасность информации, как составляющая информационной безопасности, включает в себя защиту информации и информационных ресурсов от несанкционированного доступа, искажения, уничтожения, установление режима информации в зависимости от ее содержания, обеспечение защиты сведений, составляющих государственную тайну, иной информации ограниченного доступа.

Обеспечение информационной безопасности в большинстве случаев связано с комплексным решением трех задач. Именно доступность, целостность и конфиденциальность являются равнозначными составляющими информационной безопасности.

В современном мире пользователь должен обладать рядом навыков и опытом владения электронными машинами. Конечно, обычная домохозяйка вряд ли противостоит атаки группы хакеров, но и такое событие встречается крайне редко. Зачастую пользователи попадают в неприятности из-за невнимательности и небрежности. Экономия на антивирусных программах, их отключение для получения доступа к другим ресурсам, установка программного обеспечения из сомнительных источников – все это имеет шанс заразить компьютер вирусами.

Утечка или утрата информации влечет за собой материальный ущерб. В данном реферате рассмотрены вопросы, связанные с организацией защиты от утечки конфиденциальной информации. Проведена классификация существующих угроз и

каналов утечки информации, использование которых влечет серьезные последствия для предприятия.

Существуют каналы утечки информации, образующиеся за счет:

-перехвата электромагнитных излучений и наводок, применения подслушивающих устройств, хищения и копирования носителей информации;

-наблюдения за информацией в процессе обработки с целью ее запоминания;

-чтения остаточной информации, незаконного подключения специальной регистрирующей аппаратуры к устройствам системы или линиям связи;

-злоумышленного вывода из строя механизмов защиты;

-злоумышленного изменения программ, несанкционированного получения информации путем подкупа или шантажа должностных лиц соответствующих служб; получения информации путем подкупа и шантажа сотрудников, знакомых, обслуживающего персонала или родственников, знающих о роде деятельности.

Определено, что проблему утечки информации нельзя решить каким-либо одним способом. Необходимо создание организационно-технической системы, позволяющей перекрыть каналы утечки конфиденциальной информации. Основными составляющими такой системы являются политика безопасности, работа с персоналом, сервисы безопасности. Рассмотрены способы предотвращения утечки конфиденциальной информации: организационные, правовые и технические мероприятия.

Для блокировки каналов от утечек информации могут применяться следующие способы: шумовые генераторы, поиск закладок, ограничение доступа, маскирование, шифрование, контроль доступа, криптозащиту.

Фонд региональных социальных программ «Наше будущее» — некоммерческая организация, декларирующая своей целью развитие социального предпринимательства в России.

Помимо финансовой и организационной помощи, фонд предоставляет социальным предпринимателям правовую, консультационную и информационную поддержку.

Фондом региональных социальных программ «Наше будущее» для получения необходимых сведений о претендентах на финансированиебыл создан сайт

«Конкурс социальный предприниматель».

Целью создания данного сайта Фондом «Наше будущее» является предоставление физическим лицам (пользователям) необходимых сведений о деятельности Компании и информирование об услугах (продуктах), предоставляемых Компанией. Сведения на сайте в большей степени носят информационный характер.

Физическую защиту конфиденциальной информации в фонде «Наше будущее» осуществляет служба безопасности.

В фонде «Наше будущее» организована система контроля и управления доступом. Она подразумевает физическую и сетевую охрану. К первой относятся охранники, всякого рода замки, которые организуют пропускной режим в здание, фиксируют время входа и выхода сотрудников. Аналогичной защиты требуют и информационные системы: замками в ней становятся логины и пароли, а сторожами - администраторы и специальные программные продукты.

Для обеспечения защиты конфиденциальной информации в Фонде «Наше будущее» создана служба защиты информации.

В фонде «Наше будущее» предусмотрено применение продукта Network Access Control (NAC).

В качестве защиты от вирусных программ в Фонде «Наше будущее» используется Kaspersky Anti-Virus.

Список использованных источников

1. О некоторых вопросах информационной безопасности Российской Федерации: Указ Президента РФ от 22 мая 2015 г. № 260 // Рос. газ. – 2015. – № 111.
2. Доктрина информационной безопасности Российской Федерации: утв. Президентом РФ 05 декабря 2016 г. № 646.
3. Алексенцев А.И. Сущность и соотношение понятий «защита информации», «безопасность информации», «информационная безопасность» // Безопасность информационных технологий. – 2013. – № 1.
4. Антенны и фидеры. Передача информации по каналам связи. Контроль и измерения в технике связи / ред. С.В. Бородич. - М.: НИИР, 2015. - 100 с.
5. Атаманов Г. А. Информационная безопасность: сущность и содержание // Бизнес и безопасность в России. – 2014. – № 47.

6. Бузов, Г. А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. - Москва: Наука, 2014. - 594 с.
7. Корюкова, А.А. Основы научно-технической информации / А.А. Корюкова, В.Г. Дера. - М.: Высшая школа, 2016. - 224 с.
8. Ласовская Н.Ф. Основные составляющие национальной безопасности современной России // Историческая и социально-образовательная мысль. – 2016. – № 4.
9. Малинин В.Б. Правовое регулирование информации // Ленинградский юридический журнал. – 2015. – № 3.
10. Панин Д.Н., Михайлов В.И. Исследование блока полосового и режекторного фильтров на основе операционных усилителей с пьезоэлектрическим резонатором // Радиолокация, навигация, связь: сборник трудов XXIV Международной научно-технической конференции (17-19 апреля 2018 г.). Том 5. – Воронеж: ООО «Вэлборн», 2018. – С. 32 -36.
11. Панченко Е. М., Каверин В. В., Бабанских В. А. Проблемы защиты объектов вычислительной техники от утечки информации по каналам побочных электромагнитных излучений и наводок в современных условиях // Известия Южного федерального университета. Технические науки. №7. 2015. С. 45-48.
12. Панченко Е. М., Платонов Б. Ф., Суздалев Д. В. Некоторые особенности контроля защиты объектов информатизации от утечки информации по каналам несанкционированного доступа (НСД) к информации в ходе их аттестационных испытаний и проводимых контрольных проверок // Известия Южного федерального университета. Технические науки. №6. 2016. С. 35-39.
13. Терещенко Л.К. Информационная безопасность органов исполнительной власти на современном этапе // Журнал российского права. – 2015. – № 8.
14. Угрозы информационной безопасности [Электронный ресурс] – Режим доступа: https://www.antimalware.ru/threats/information-security-threats. (дата обращения: 27.08.2020).
15. Предотвращение утечек данных - DLP [Электронный ресурс] – Режим доступа: http://allta.com.ua/nashi-resheniya/informacionnaya-bezopasnost/dlp-systems(дата обращения: 27.08.2020).
16. Вредоносные майнеры - новая угроза информационной безопасности [Электронный ресурс] – Режим доступа: https://www.anti-malware.ru/analytics/Threats_Analysis/cryptojacking-new-threat(дата обращения: 27.08.2020).
17. Информационная безопасность вчера и сегодня [Электронный ресурс] – Режим доступа: https://moluch.ru/archive/185/47410(дата обращения: 27.08.2020).

18. Фонд Наше Будущее [Электронный ресурс] – Режим доступа: http://www.nb-fund.ru/ (дата обращения: 7.09.2020).