НЕГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «РОССИЙСКАЯ АКАДЕМИЯ АДВОКАТУРЫ И НОТАРИАТА»

ТВОРЧЕСКОЕ ЗАДАНИЕ

По дисциплине:

Актуальные проблемы права

На тему:

«Понятие «информационная безопасность», проблемы ее обеспечения на предприятии»

Выполнила:

Студентка 1 курса магистратуры

Сорокина Ольга Вячеславовна

Проверил:

_____

Москва, 2018

Оглавление

Информационная безопасность. 2
1. Основные категории информационной безопасности 3
2. Информационная безопасность предприятия. 5
2.1 Проблемы обеспечения информационной безопасности предприятия 6
3. Задачи информационной безопасности предприятия. 8
Заключение 10
Список литературы 11

Информационная безопасность.

Характерной чертой современного общества является его информатизация – активная разработка и внедрение во все сферы человеческой деятельности информационных технологий и средств. Информация и информационные ресурсы становятся одним из решающих факторов развития личности, общества и государства. Широкие возможности компьютеров и информационных технологий позволяют автоматизировать процессы мониторинга и управления государственными, экономическими, социальными, оборонными и другими объектами и системами, получать, накапливать, обрабатывать и передавать информацию об этих процессах практически с любой требуемой скоростью, в любом количестве.

Все это дает основание утверждать, что информатизация играет сегодня решающую позитивную роль в развитии человечества, что информационное общество объективно неизбежно. Но история учит нас тому, что многие достижения научно-технической мысли использовались не только во благо людей. Достаточно вспомнить достижения ядерной физики – атомное оружие, опто-электроники – лазерное оружие, химии – отравляющие газы, биологии – биологическое оружие и т. д. Всегда находились силы, которые стремились использовать в своих интересах открытия в научно-технической сфере.

Сегодня у определенных субъектов (коалиций, государств, организаций, личностей) возникает стремление единолично обладать информационными ресурсами, средствами и технологиями и использовать их для удовлетворения своих интересов и противодействия интересам вероятных конкурентов в экономическом, коммерческом и даже военном противоборстве. Информация и информационные технологии при этом начинают выступать в качестве объектов угроз, что порождает проблему информационной безопасности.

1. Основные категории информационной безопасности

Концептуальные и научно-методологические основы информационной безопасности еще только начинают разрабатываться. Первоочередной задачей при создании теории информационной безопасности следует считать формирование понятийного аппарата. Базовыми понятиями являются информационная опасность, информационная угроза и информационная безопасность.

Информационная опасность определяется двояко:

• как состояние окружающей среды или объекта, в котором существует возможность причинить им существенный ущерб или вред путем оказания воздействия на информационную сферу объекта;

• как свойство объекта, характеризующееся способностью наносить существенный ущерб другому объекту путем оказания воздействия на его информационную сферу.

В соответствии с этим **информационная безопасность** – это:

состояние объекта, когда ему путем воздействия на его информационную сферу не может быть нанесен существенный ущерб или вред;

• свойство объекта, характеризующее его способность не наносить существенного ущерба какому-либо объекту путем оказания воздействия на информационную сферу этого объекта.

Информационная угроза – угроза объекту путем оказания воздействия на его информационную сферу:

• намерение нанести (причинить) объекту существенный ущерб путем оказания воздействия на его информационную сферу;

• информационная опасность, реализация которой становится весьма вероятной;

• фактор или совокупность факторов, создающих информационную опасность объекту; такими факторами могут быть действия, поведение объектов, природные явления и т. д.

Все вышесказанное позволяет сформулировать понятие **информационной безопасности Российской Федерации** как такое состояние страны, в котором гражданам, объединениям и общественным группам граждан, обществу и государству не может быть нанесен существенный ущерб путем оказания воздействия на ее информационную сферу.

Основными *объектами информационной безопасности* являются личность (ее права и свободы), общество (его материальные и духовные ценности) и государство (его конституционный строй, суверенитет, территориальная целостность, экономика, военное дело и т. д.).

Личность – базовый элемент, ячейка общества. Без личности нет общества, но и личность вне общества существовать не может. Государство обеспечивает условия существования и личности, и общества. Государства, которые не нужны ни личности, ни обществу, не могут существовать долго и исчезают с исторической арены. Баланс взаимоотношений между личностью,

обществом и государством выступает главным условием их устойчивого развития.

Информационная безопасность личности – это состояние человека, в котором его личности не может быть нанесен существенный ущерб путем оказания воздействия на окружающее информационное пространство.

В процессе информатизации человек стал информационно «прозрачен». При наличии желания и средств любая имеющаяся информация о конкретной личности может стать доступной и быть использована в своих целях другой личностью, группой лиц, общественной группой и государством. Только незначительная часть населения способна предотвратить нежелательный доступ к своей информации. Большинство людей такой возможности не имеют и остаются беззащитными в этом плане.

Информационная безопасность общества – это состояние общества, в котором ему не может быть нанесен существенный ущерб путем воздействия на его информационную сферу. В ее основе – безопасность индивидуального, группового и массового сознания граждан при наличии информационных угроз, к которым в первую очередь следует отнести информационно-психологическое воздействие. Действие этих угроз может вызывать психоэмоциональную и социально-психологическую напряженность, искажение нравственных критериев и норм, морально-политическую дезориентацию и, как следствие, неадекватное поведение отдельных лиц, групп и масс людей. В результате таких воздействий возможны глубокие трансформации индивидуального, группового и массового сознания, негативные изменения морально-политического и социально-психологического климата в обществе.

Информационная безопасность государства – это состояние государства, в котором ему не может быть нанесен существенный ущерб путем оказания воздействия на его информационную сферу. Обеспечение информационной безопасности государства неразрывно связано с обеспечением национальной безопасности.

2. Информационная безопасность предприятия.

Всем известно высказывание «Кто владеет информацией, тот владеет миром». А кто владеет информацией о конкурентах, получает беспрецедентные преимущества в борьбе с ними. Прогресс сделал компании зависимыми от информационных систем, а вместе с этим — уязвимыми к атакам хакеров, компьютерным вирусам, человеческому и государственному фактору в такой степени, что многие владельцы бизнеса уже не могут чувствовать себя в безопасности. Вопрос информационной безопасности становится краеугольным камнем в деятельности организации, но этот же прогресс предлагает решения, способные защитить данные от внешних посягательств.

Для каждого современного предприятия, компании или организации одной из самых главных задач является именно обеспечение информационной безопасности. Когда предприятие стабильно защищает свою информационную систему, оно создает надежную и безопасную среду для своей деятельности. Например, могут появиться убытки от плохой репутации компании, от отсутствия клиентов, от затрат на возобновление стабильной работы или от потери важной информации, которой располагала данная компания. Любая утечка информации может привести к серьезным проблемам для компании — от значительных финансовых убытков до полной ликвидации. Конечно, проблема утечек появилась не сегодня, промышленный шпионаж и переманивание квалифицированных специалистов существовали еще и до эпохи компьютеризации. Но именно с появлением ПК и интернета возникли новые приемы незаконного получения информации. Если раньше для этого необходимо было украсть и вынести из фирмы целые кипы бумажных документов, то сейчас огромные объемы важных сведений можно запросто слить на флэшку, помещающуюся в портмоне, отправить по сети, прибегнув к использованию семейства руткитов, троянов, бэкдоров, кейлоггеров и ботнетов, либо просто уничтожить посредством вирусов, устроив диверсию. Чаще всего «утекают» из компаний документы финансового характера, технологические и конструкторские разработки, логины и пароли для входа в сеть других организаций. Но серьезный вред может нанести и утечка персональных данных сотрудников. Особенно это актуально для западных стран, где судебные иски из-за таких утечек нередко приводят к огромным штрафам, после выплаты которых компании терпят серьезные убытки.

2.1 Проблемы обеспечения информационной безопасности предприятия.

Аналитический центр InfoWatch опубликовал данные по утечке данных в России за 2016 год. Согласно исследованию, СМИ обнародовали 213 случаев утечек информации из российских госорганов и компаний, что составляет 14% от общемирового количества утечек. Самые частые случаи — это утечка платежной информации и персональных данных — 80%. В 68% случаев виновными оказываются сотрудники организаций, и только в 8% — руководство. По сравнению с 2015 годом количество утечек выросло на 89%. На сегодня Россия занимает второе после США место в списке стран, наиболее сильно страдающих от утечек информации.

- ***Невнимательность и халатность сотрудников***.

Угрозу информационной безопасности компании, как ни странно, могут представлять вполне лояльные сотрудники и не помышляющие о краже важных данных. Непредумышленный вред конфиденциальным сведениям причиняется по простой халатности или неосведомленности работников. Всегда есть возможность того, что кто-нибудь откроет фишинговое письмо и внедрит вирус с личного ноутбука на сервер компании. Или, например, скопирует файл с конфиденциальными сведениями на планшет, флэшку или КПК для работы в командировке. И ни одна компания не застрахована от пересылки невнимательным сотрудником важных файлов не по тому адресу. В такой ситуации информация оказывается весьма легкой добычей.

- ***Использование пиратского ПО.***

Иногда руководители компаний пытаются сэкономить на покупке лицензионного ПО. Но следует знать, что нелицензионные программы не дают защиты от мошенников, заинтересованных в краже информации с помощью вирусов. Обладатель нелицензионного ПО не получает технической поддержки, своевременных обновлений, предоставляемых компаниями-разработчиками. Вместе с ним он покупает и вирусы, способные нанести вред системе компьютерной безопасности.

- ***Вирусы***.

Одной из самых опасных на сегодняшний день угроз информационной безопасности являются компьютерные вирусы. Это подтверждается многомиллионным ущербом, который несут компании в результате вирусных атак. В последние годы существенно увеличилась их частота и уровень ущерба. По мнению экспертов, это можно объяснить появлением новых каналов проникновения вирусов. На первом месте по-прежнему остается почта, но, как показывает практика, вирусы способны проникать и через программы обмена сообщениями, такие как ICQ и другие. Увеличилось и количество объектов для возможных вирусных атак. Если раньше атакам подвергались в основном серверы стандартных веб-служб, то сегодня вирусы

3. Задачи информационной безопасности предприятия.

На данный момент сформулировано три базовых задачи, которые должна обеспечивать информационная безопасность:

- Целостность данных — защита от сбоев, ведущих к потере информации, а также защита от незаконного создания или уничтожения данных. Примером нарушения целостности данных является повреждение бухгалтерских баз, в дальнейшем это повлечет за собой последствия, которые определенно станут негативными для компании.
- Конфиденциальность информации — незаконное разглашение, утечка, повреждение информации;
- Доступность информации для всех пользователей — отказ в обслуживании или услугах, которые могут быть вызваны вирусной активностью или действиями злоумышленников.

Нарушение одного из этих аспектов может привести к невозможности нормальной работы предприятия. На наличие любого из нарушений могут повлиять и внутренние, и внешние угрозы. Учитывая сегодняшнее развитие информационного общества, можно сделать вывод о тенденции к росту количества угроз безопасности.

Полноценная информационная безопасность компаний предполагает постоянный контроль всех существенных событий и состояний, которые влияют на надежность защиты информации. Причем, защита обязана осуществляться постоянно и охватывать весь жизненный цикл данных, то есть от ее поступления или создания до уничтожения или утраты важности и актуальности.

Основными факторами, оказывающими влияние на защиту информации и данных на предприятии, являются:

- Приумножение сотрудничества компании с партнерами;
- Автоматизация бизнес-процессов;
- Тенденция к росту объемов информации предприятия, которая передается по доступным каналам связи;
- Тенденция к росту компьютерных преступлений.

Информационная защита предприятия определяется целым сочетанием предпринимаемых мер, которые направлены на безопасность важной информации. Эти меры можно разделить на две группы:

- Организационные меры;
- Технические меры.

Организационные меры заключаются в формальных процедурах и правилах работы с важной информацией, информационными сервисами и средствами

защиты. Технические меры включают в себя использование программных средств контроля доступа, мониторинг утечек и краж информации, антивирусную защиту, защиту от электромагнитных излучений и т. д.

Задачи систем информационной безопасности компании многогранны. К примеру, это обеспечение надежного хранения данных на различных носителях; защита информации, передаваемой по каналам связи; ограничение доступа к некоторым данным; создание резервных копий и другое.

Полноценное обеспечение информационной безопасности компании реально только при правильном подходе к защите данных.

Заключение.

Информатизация общества порождает проблемы информационной безопасности, главные из которых – проблема информационных войн и информационного терроризма. В современном обществе информационная безопасность является важнейшим компонентом национальной безопасности. От нее в значительной степени зависит уровень экономической, оборонной, социальной, политической и других видов безопасности.

В условиях постоянного роста количества известных и появления новых видов информационных угроз перед крупными предприятиями всё чаще встаёт задача обеспечения надёжной защиты корпоративных сетей от вредоносных программ и сетевых атак.

Информационная безопасность предприятия - это состояние защищённости корпоративных данных, при которой обеспечивается их конфиденциальность, целостность, аутентичность и доступность. Обеспечение информационной безопасности предприятия возможно только при системном и комплексном подходе к защите. В системе ИБ должны учитываться все актуальные компьютерные угрозы и уязвимости.

Полноценная информационная безопасность предприятий и организаций подразумевает непрерывный контроль в реальном времени всех важных событий и состояний, влияющих на безопасность данных. Защита должна осуществляться круглосуточно и круглогодично и охватывать весь жизненный цикл информации - от её поступления или создания до уничтожения или потери актуальности.

Список литературы

1. Информационная безопасность. Защита информации — [Электронный ресурс] — Режим доступа. — URL: http://all-ib.ru/
2. Определение информационной безопасности — [Электронный ресурс] URL: http://www.itspecial.ru/opredelenie_informacionnoi_bezopasnosti.html
3. Угрозы информационной безопасности в АС — [Электронный ресурс] — Режим доступа. — URL: http://asher.ru/security/book/its/05
4. Comparison of antivirus software — [Электронный ресурс] — Режим доступа: URL: http://en.wikipedia.org/wiki/Comparison_of_antivirus_software
5. Информационная безопасность предприятия: ключевые угрозы и средства защиты — [Электронный ресурс] — Режим доступа: URL:https://www.kp.ru/guide/informatsionnaja-bezopasnost-predprijatija.html
6. Поляков Андрей Владимирович: Проблематика информационной безопасности в экономических научных направлениях// Современные технологии управления. ISSN 2226-9339. — №10 (10). Номер статьи: 1003. Дата публикации: 2011-10-08 — [Электронный ресурс] — Режим доступа: http://sovman.ru/article/1003/
7. Новые информационные коммуникационные технологии в образовании / В.А. Трайнев, В.Ю. Теплышев, И.В. Трайнев. - 2-е изд. - М.: Издат.-торговая корпорация "Дашков и К°", 2014. - 320 с. [Электронный ресурс] — Режим доступа: URL:http://www.ozon.ru/context/detail/id/4136468/