

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Бервецкая Ю.А.
Научный руководитель: Манжула Т.Ю.

*ГО ВПО «Донецкий национальный университет экономики и торговли
имени Михаила Туган-Барановского»*

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОВРЕМЕННЫХ УСЛОВИЯХ

Информационные технологии используются повсеместно, и многие уже не могут представить свою жизнь без них: социальные сети, мессенджеры, интернет-магазины, онлайн-банкинг — все эти средства связи и коммуникаций мы используем, и все эти точки доступа потенциально уязвимы. С развитием технологий все сложнее становится защита личных данных. В этой статье мы рассмотрим возможности решения данной проблемы.

В современном мире электронные почты или аккаунты в социальных сетях подвергаются взлому злоумышленников, которые не останавливаются на одном пользователе. Десяткам людей рассылается спам и вредоносные программы. Стоит лишь открыть документ и компьютер заражается вредоносным программным обеспечением.

Информационная безопасность при работе с мобильными банковскими приложениями

Сегодня клиенты общаются с банками в рамках следующих приложений:

- банк-клиент или онлайн-банкинг через персональные компьютеры;
- мобильные онлайн приложения;
- социальные сети и мессенджеры.

Советы клиентам тут следующие:

- не использовать пароли в интернет и онлайн-банкинг, которые уже задействованы в других сервисах.
- тщательно проверять, куда и кому вы платите.
- не посылать данные своей банковской карты, логины и пароли в онлайн-сервисы на непроверенные сайты.
- не хранить средства на той карте, с которой вы рассчитываетесь через интернет.
- не использовать платежи на посторонних сайтах.

Безопасность информации — состояние защищенности данных, при которых обеспечены их доступность, конфиденциальность и целостность.

Для защиты информации информация должна быть:

1. достаточно защищена от взлома извне;
2. оперирована достаточно образованным лицом;
3. недоступна для неуполномоченных лиц [1].

Защита информации — это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Многие организации выстраивают собственные системы информационной безопасности, проводят проверки и анализ защищенности данных. Это касается как персональных данных клиентов и персонала, так и информации о текущей деятельности, финансовом состоянии.

Современные организации используют требования международных стандартов для построения систем менеджмента информационной безопасности и используют лучшие мировые практики.

Вне зависимости от того, в каком виде информация сохраняется, как используется, нужно реализовывать адекватные меры защиты. Любой руководитель должен объективно оценивать текущее состояние информационных систем, видеть и понимать существующие информационные проблемы.

Для этого в организации должно проводиться обучение ответственных лиц и пользователей определенным моментам работы с данными. Устанавливаются программные средства защиты, программное обеспечение, регулярное обновление антивирусных программ, шифрование данных.

Все зловредные программы делятся на несколько типов. В первую очередь это троянские программы, это программы, которые устанавливаются на ПК, они никак себя не проявляют, их очень сложно обнаружить, основная их задача состоит в том, чтобы собирать информацию о пользователе с помощью считывания информации: пароли, пин-код карточки, личная информация все это переходит мошеннику с помощью данной программы. Другой тип вредоносных программ это шифровальщики. После внедрения этого вируса на ваш ПК, программа превращает наше устройство в «кирпич», то есть вся та информация превращается в набор бесполезных цифр и букв, после чего обычно приходит сообщение, в котором злоумышленник предлагает вам за деньги выдать ключ, который позволит эту информацию расшифровать и вернуть. Еще одна категория вредоносных программ это так называемые программы-зомби. После ее внедрения на ПК пользователя, мошенник может контролировать наше устройство извне. Это часто используется для того, чтобы рассылать спам или для компьютерных атак, когда огромное количество сетей посылают запросы на социальную сеть, почтовый сервис или магазин, от того что они посылаются одновременно сайт не выдерживает и прекращает свою работу. Компьютерный вирус — вид вредоносного программного обеспечения. Оно способно создавать собственные копии, внедряться в код других программ, загрузочные секторы или системные области памяти, а также распространять собственные копии по различным каналам связи[2].

Защитить важную для себя информацию может любой человек. Для этого достаточно не игнорировать некоторые угрозы. Так, например, не использовать простые пароли. Пароли «0000» на вашем телефоне или «parol1» на почте

вполне могут привести к утере важных для вас данных. Чтобы ваш пароль был надежен, в идеале он должен состоять из букв и цифр, иметь больше 8 знаков, содержать как заглавные, так и прописные буквы, а так же не совпадать ни с одним словарным словом [1].

Пользователям необходимо использовать только надежные устройства хранения данных. Если устройство чужое и вы о нем ничего не знаете, есть риск подключить к компьютеру устройство с вирусом.

Для того чтобы обезопасить пользование компьютером, необходимо также должны помнить о некоторых моментах работы в Интернете. Ни в коем случае нельзя сообщать в Интернете свое имя, номер телефона, номер кредитной карты, адрес проживания, пароль.

Используя различные способы защиты по максимуму, пользователи создают собственную систему информационной безопасности, позволяющую сохранить свои данные, снизить до минимума риски несанкционированного доступа к различного рода сведениям, имеющим важное значение в жизни.

Список литературы:

1. Лободина, А.С. Информационная безопасность / А.С. Лободина, В.В. Ермолаева. — Текст: непосредственный, электронный // Молодой ученый. — 2017. — № 17 (151). — С. 17-20. — URL: <https://moluch.ru/archive/151/42898/> (дата обращения: 27.04.2020).

2. Базовая информация о информационной безопасности [Электронный ресурс] // Интернет-портал – URL: <http://bezopasnik.org/article/1.htm> (Дата обращения: 27.04.2020)

3. Базовая информация о информационной безопасности [Электронный ресурс] // Интернет- портал – URL: <http://bezopasnik.org/article/1.htm> (дата обращения 27.04.2020)

Гонтарь Л.Е.

Научный руководитель: Лутай А.П., к.э.н., доцент

*ГО ВПО «Донецкий национальный университет экономики и торговли
имени Михаила Туган-Барановского»*

СОСТАВЛЯЮЩИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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:

1. Обеспечением доступности информации.
2. Обеспечением целостности информации.
3. Обеспечением конфиденциальности информации.

Именно доступность, целостность и конфиденциальность являются

равнозначными составляющими информационной безопасности.

Информационные системы создаются для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, то это, очевидно, наносит ущерб всем пользователям.

Роль доступности информации особенно проявляется в разного рода системах управления – производством, транспортом и т. п. Менее драматичные, но также весьма неприятные последствия – и материальные, и моральные – может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей, например, продажа железнодорожных и авиабилетов, банковские услуги, доступ в информационную сеть Интернет и т. п.

Доступность – это гарантия получения требуемой информации или информационной услуги пользователем за определенное время.

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 уместной является поговорка: "Дорога ложка к обеду".

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 и др.

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

Так, ошибка в управляющей программе приведет к остановке управляемой системы, неправильная трактовка закона может привести к его нарушениям, точно также неточный перевод инструкции по применению лекарственного препарата может нанести вред здоровью. Все эти примеры иллюстрируют нарушение целостности информации, что может привести к катастрофическим последствиям. Именно поэтому целостность информации выделяется в качестве одной из базовых составляющих информационной безопасности.

Целостность – гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений.

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 лишено возможности составить представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные и технические проблемы.

Конфиденциальная информация есть практически во всех организациях. Это может быть технология производства, программный продукт, анкетные данные сотрудников и др. Применительно к вычислительным системам в обязательном порядке конфиденциальными данными являются пароли для доступа к системе.

Конфиденциальность – гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена.

Нарушение каждой из трех категорий приводит к нарушению информационной безопасности в целом. Так, нарушение доступности приводит к отказу в доступе к информации, нарушение целостности приводит к фальсификации информации и, наконец, нарушение конфиденциальности приводит к раскрытию информации.

Подводя итоги нужно отметить, выделение этих категорий в качестве базовых составляющих информационной безопасности обусловлено необходимостью реализации комплексного подхода при обеспечении режима информационной безопасности. Кроме этого, 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).

Данилов А.В.

Научный руководитель: Пророчук Ж.А.

*ГО ВПО «Донецкий национальный университет экономики и торговли
имени Михаила Туган-Барановского»*

ИСПОЛЬЗОВАНИЕ ПРОГРАММНЫХ СРЕДСТВ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ

Наша современность не представляется без использования небывалых возможностей информационных технологий. Однако свои краеугольные камни проявились в защите конфиденциальности информационной системы, внедренных информационных технологиях. Ключевую роль в обеспечении безопасности информационной системы играют человеческие, нормативные (законодательные) и технологические факторы [1]. «Согласно отчёту,

опубликованному Генпрокуратурой, и расширенным данным, которые были предоставлены ведомством по просьбе «АГ», в 2017 г. число преступлений в сфере информационно-телекоммуникационных технологий увеличилось на 37% (с 65 949 в 2016 г. до 90 587 в 2017 г.). При этом доля таких преступлений от числа всех зарегистрированных в России составляет 4,4%: это почти каждое 20-е преступление» [2]. «Самые частые случаи — это утечка платежной информации и персональных данных — 80%. В 68% случаев виновными оказываются сотрудники организаций и только в 8% — руководство» [3].

Это в очередной раз подтверждает необходимость полного контроля всех действий пользователей на компьютерах и блокировки нежелательных действий. Кроме того, важным фактором являются затраты на защиту — они не должны превышать размера возможного ущерба.

В этой связи перед компаниями встает вопрос выбора методов и инструментов для обеспечения защиты корпоративной информации [4]. А поскольку значение этой проблематики и на сегодняшний день не теряет своей актуальности, выбор этот оказывается сложным. В качестве примеров средств борьбы за информационную безопасность можно привести следующие полезные программы: Nessus, VirusTotal, Secunia PSI, Autoruns, CrowdInspect, Should I Remove It? и Solutio, ShieldsUp, Malwarebytes и HijackThis, NoScript и ScriptSafe, CCleaner, Pandora Recovery, WDO [5]. Российская компания DEAC, специализирующаяся на предоставлении услуг по защите информации, предлагает комплекс эффективных решений по защите данных [2]: резервное копирование данных Backup-as-a-Service (BaaS) и их хранение в облаке DEAC на базе одного или нескольких дата-центров; высокого уровня защита данных, расположенных на инфраструктуре DEAC, вне зависимости от их расположения — как в России, так и в Европе — достигается дополнительно при помощи системы защиты от DDoS-атак; разработка плана аварийного восстановления (disaster recovery) ИТ-системы с учётом особенностей бизнеса каждой компании, анализируя риски и определяя важнейшие вопросы безопасности на межгосударственном уровне [3].

В данной работе предлагается более подробно ознакомиться со специальными возможностями программы «Lanagent enterprise», поскольку универсальные возможности ее поистине широки, и несмотря на высокую потребность в подобных программах, конкурентов на рынке России и стран СНГ пока не существует.

Первоначальная версия продукта «Lanagent enterprise» была разработана в 2005 году, а в настоящее время усовершенствована и интегрирована под новый и более функциональный уровень.

Началу процесса создания программы «Lanagent enterprise» послужило неоднократное обращение руководителей различных компаний к разработчикам с различного рода вопросами и требованиями. Наиболее распространенными и острыми оказались вопросы, связанные с защитой утечки информации, контроля работы пользователей и обеспечения рациональности использования рабочего времени сотрудников. Общепринятый подход к разрешению подобных вопросов подразумевает многоступенчатое проведение

обследования системы, аудита состояния информационной безопасности, разработку новой или корректировку существующей политики безопасности. Вследствие этого возникает потребность большинство этих мероприятий проводить с помощью одного универсального программного продукта. Сублимацией поставленных задач и стала программа «Lanagent enterprise», представляющая собой комплексную систему по контролю рабочего времени сотрудников и обеспечению информационной безопасности компании [6].

Эффективность и целесообразность использования «Lanagent enterprise» проверена временем: в странах СНГ и в России она активно применяется с 2005 года, среди многочисленных пользователей – компании «Транснефть», «Роснефть». Разработчик имеет лицензии ФСТЭК России на разработку средств защиты информации, поэтому использование этой программы абсолютно законно, а приобретённая лицензия бессрочна. Одним из важных достоинств программы является удобство и простота в использовании. Кроме того, «Lanagent enterprise» даёт возможность скрытого дистанционного режима наблюдения и анализа действий пользователя за компьютером, контролируя эффективность распределения его рабочего времени. Простой и удобный интерфейс вместе с тем органично объединяет в себе широкий спектр специальных возможностей. Использование данной программы не предусматривает обязательное наличие каких-либо углубленных навыков в сфере компьютерных технологий. Также не требуется применения дополнительного оборудования или специального программного обеспечения: установка и детальная настройка конфигураций осуществляются дистанционно в кратчайшие сроки, максимум до двух дней в масштабной компании, и не вызывает сложностей с производительностью даже на «слабых» компьютерах [6].

Однако среди недостатков «Lanagent enterprise» следует отметить нехватку возможностей отражать графическое представление информации в виде диаграмм. Некоторые неудобства также связаны с ограничением сроков процесса передачи информации с компьютеров пользователей серверу, что в некоторой степени лимитирует контроль в реальном времени.

Таким образом, реалии сегодняшнего времени предъявляют определенные требования при работе с информационными технологиями. И решения проблемы безопасности информационной системы среди подобных требований оказываются на первом месте. Немаловажной задачей является необходимость полного контроля эффективности работы сотрудников предприятия за компьютером. Панацеей решения этой проблемы стало создание и постоянное усовершенствование «Lanagent enterprise». Данный программный продукт может быть рекомендован компаниям для повышения производительности труда своих сотрудников.

Список литературы:

1. Ахмедова А. Защита информации от внутренних угроз [Электронный ресурс]. – Режим доступа: <<https://cyberleninka.ru/article/n/zaschita-informatsii-ot-vnutrennih-ugroz-1/viewer>>.

2. Киберпреступлений становится все больше, однако их раскрываемость уменьшается [Электронный ресурс]. – Режим доступа: <<https://www.advgazeta.ru/novosti/kiberprestupleniy-stanovitsya-vse-bolshe-odnako-ikh-raskryvaemost-umenshaetsya/>>.

3. Информационная безопасность предприятия: ключевые угрозы и средства защиты [Электронный ресурс]. – Режим доступа: <<https://www.kp.ru/guide/informatsionnaja-bezopasnost-predpriyatija.html>>.

4. Домбровская Л., Яковлева Н., Стахно Р. Современные подходы к защите информации, методы, средства и инструменты защиты [Электронный ресурс]. – Режим доступа: <<https://cyberleninka.ru/article/n/sovremennye-podhody-k-zaschite-informatsii-metody-sredstva-i-instrumenty-zaschity/viewer>>.

5. Программное обеспечение для информационный безопасности [Электронный ресурс]. – Режим доступа: <<https://netoscope.ru/ru/tips/686/>>.

6. Программа Lanagent enterprise – контроль рабочего времени сотрудников / обеспечение информационной безопасности [Электронный ресурс]. – Режим доступа: <https://lanagent.ru/lanagent_ent-about.html>.

Дмитриенко А.В.

ГПОУ «Донецкий техникум промышленной автоматики»

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Когда мы говорим о безопасности сети, поиске совершенных мер защиты, забываем о том, что большинство утечек информации происходит благодаря человеческому фактору - небрежность сотрудников, порой психологическая неустойчивость, доверчивость могут привести к фатальной потере данных. Пока администраторы сетей ставят межсетевые экраны, устройства идентификации, средства шифрования, системы обнаружения сетевых атак, злоумышленники проникают в сеть с помощью рядовых, ничего не подозревающих, пользователей. Пожалуй, чаще всего для получения доступа к сети применяется метод, именуемый социальной инженерией - и на него же зачастую обращают меньше всего внимания. Вариантов использования социальной инженерии существует огромное количество, поэтому рядовые пользователи должны быть ознакомлены хотя бы с основными из них.

Понятие "социальная инженерия" обозначает любые варианты психологического воздействия на человека, такие как введение в заблуждение, игра на чувствах человека, в том числе и шантаж. Социальная инженерия - термин, используемый злоумышленниками для обозначения несанкционированного доступа к информации, не связанного со взломом программного обеспечения. Цель - обмануть пользователей для получения доступа к системе или информации, которая поможет нарушить безопасность системы.

Одной из основных причин распространения социальной инженерии как метода атаки является дешевизна этого вида нападения, поскольку атакующий может и не быть специалистом в сфере информационных технологий. Существенным фактором является также и то, что при использовании методов социальной инженерии результат нередко достигается гораздо быстрее, чем, если бы был использован иной метод для нападения.

Виды атак

Претекстинг - это набор действий, отработанных по определенному, заранее составленному сценарию, в результате которого жертва может выдать какую-либо информацию или совершить определенное действие. Чаще всего данный вид атаки предполагает использование голосовых средств, таких как Skype, телефон и т.п.

Для использования этой техники злоумышленнику необходимо изначально иметь некоторые данные о жертве (имя сотрудника, должность, название проектов, с которыми он работает, дату рождения). Злоумышленник изначально использует реальные запросы с именем сотрудников компании и, после того как войдет в доверие, получает необходимую ему информацию.

Фишинг – техника интернет-мошенничества, направленная на получение конфиденциальной информации пользователей – авторизационных данных различных систем. Основным видом фишинговых атак является поддельное письмо, отправленное жертве по электронной почте, которое выглядит как официальное письмо от платежной системы или банка. В письме содержится форма для ввода персональных данных (пин-кодов, логина и пароля, данных банковской карты) или ссылка на web-страницу, где располагается такая форма. Причины доверия жертвы подобным страницам могут быть разные: блокировка аккаунта, поломка в системе, утеря данных и прочее.

Троянский конь – это техника основывается на любопытстве, страхе или других эмоциях пользователей. Злоумышленник отправляет письмо жертве посредством электронной почты, во вложении которого находится «обновление» антивируса, ключ к денежному выигрышу или компромат на сотрудника. На самом же деле во вложении находится вредоносная программа, которая после того, как пользователь запустит ее на своем компьютере, будет использоваться для сбора или изменения информации злоумышленником.

Кви про кво (услуга за услугу) – данная техника предполагает обращение злоумышленника к пользователю по электронной почте или корпоративному телефону. Злоумышленник может представиться, например, сотрудником технической поддержки и информировать о возникновении технических проблем на рабочем месте. Далее он сообщает о необходимости их устранения. В процессе «решения» такой проблемы, злоумышленник подталкивает жертву на совершение действий, позволяющих атакующему выполнить определенные команды или установить необходимое программное обеспечение на компьютере жертвы.

Дорожное яблоко – этот метод представляет собой адаптацию троянского коня и состоит в использовании физических носителей (CD, флэш-накопителей). Злоумышленник обычно подбрасывает такой носитель в

общедоступных местах на территории компании (парковки, столовые, рабочие места сотрудников, туалеты). Для того чтобы у сотрудника возник интерес к данному носителю, злоумышленник может нанести на носитель логотип компании и какую-нибудь подпись. Например, «данные о продажах», «зарплата сотрудников», «отчет в налоговую» и другое.

Обратная социальная инженерия - данный вид атаки направлен на создание такой ситуации, при которой жертва вынуждена будет сама обратиться к злоумышленнику за «помощью». Например, злоумышленник может выслать письмо с телефонами и контактами «службы поддержки» и через некоторое время создать обратимые неполадки в компьютере жертвы. Пользователь в таком случае позвонит или свяжется по электронной почте со злоумышленником сам, и в процессе «исправления» проблемы злоумышленник сможет получить необходимые ему данные.

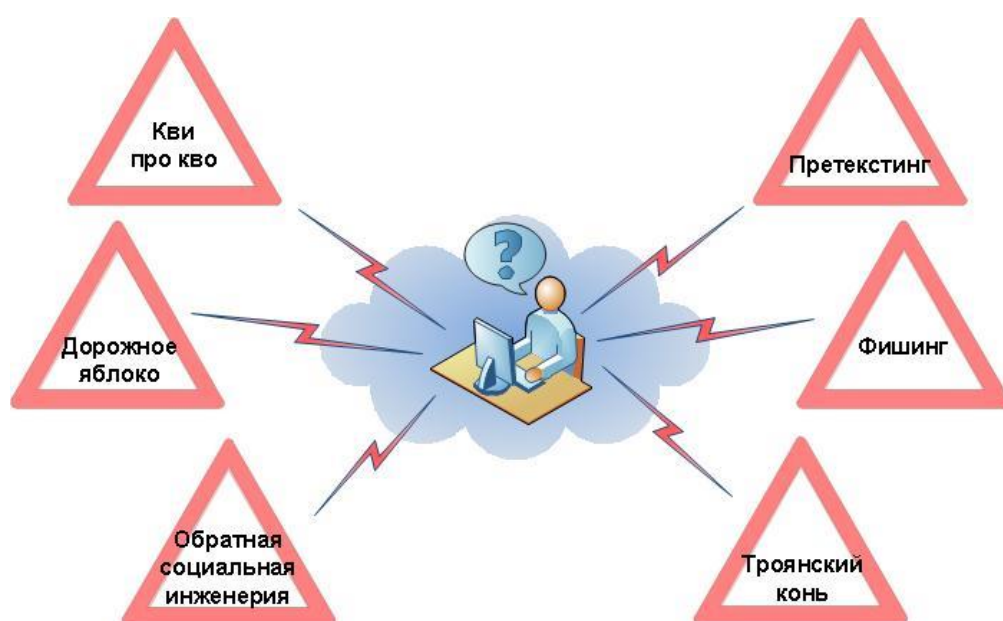


Рисунок 1 – Основные типы социальной инженерии

Меры противодействия

Основным способом защиты от методов социальной инженерии является обучение сотрудников. Все работники компании должны быть предупреждены об опасности раскрытия персональной информации и конфиденциальной информации компании, а также о способах предотвращения утечки данных. Кроме того, у каждого сотрудника компании, в зависимости от подразделения и должности, должны быть инструкции о том, как и на какие темы можно общаться с собеседником, какую информацию можно предоставлять для службы технической поддержки, как и что должен сообщить сотрудник компании для получения той или иной информации от другого сотрудника.

Можно выделить следующие правила:

- Пользовательские учетные данные являются собственностью компании.

Всем сотрудникам в день приема на работу должно быть разъяснено то,

что те логины и пароли, которые им выдали, нельзя использовать в других целях (на web-сайтах, для личной почты и т.п.), передавать третьим лицам или другим сотрудникам компании, которые не имеют на это право. Например, очень часто, уходя в отпуск, сотрудник может передать свои авторизационные данные своему коллеге для того, чтобы тот смог выполнить некоторую работу или посмотреть определенные данные в момент его отсутствия.

- Необходимо проводить вступительные и регулярные обучения сотрудников компании, направленные на повышения знаний по информационной безопасности.

Проведение таких инструктажей позволит сотрудникам компании иметь актуальные данные о существующих методах социальной инженерии, а также не забывать основные правила по информационной безопасности.

- Обязательным является наличие регламентов по безопасности, а также инструкций, к которым пользователь должен всегда иметь доступ. В инструкциях должны быть описаны действия сотрудников при возникновении той или иной ситуации.

Например, в регламенте можно прописать, что необходимо делать и куда обращаться при попытке третьего лица запросить конфиденциальную информацию или учетные данные сотрудников. Такие действия позволят вычислить злоумышленника и не допустить утечку информации.

- На компьютерах сотрудников всегда должно быть актуальное антивирусное программное обеспечение.

На компьютерах сотрудников также необходимо установить брандмауэр.

- В корпоративной сети компании необходимо использовать системы обнаружения и предотвращения атак.

Также необходимо использовать системы предотвращения утечек конфиденциальной информации. Все это позволит снизить риск возникновения фишинговых атак.

- Все сотрудники должны быть проинструктированы, как вести себя с посетителями.

Необходимы четкие правила для установления личности посетителя и его сопровождения. Посетителей всегда должен сопровождать кто-то из сотрудников компании. Если сотрудник встречает неизвестного ему посетителя, он должен в корректной форме поинтересоваться, с какой целью посетитель находится в данном помещении и где его сопровождение. При необходимости сотрудник должен сообщить о неизвестном посетителе в службу безопасности.

- Необходимо максимально ограничить права пользователя в системе.

Например, можно ограничить доступ к web-сайтам и запретить использование съемных носителей. Ведь, если сотрудник не сможет попасть на фишинговый сайт или использовать на компьютере флеш-накопитель с «троянской программой», то и потерять личные данные он также не сможет.

Вывод. Исходя из всего перечисленного, можно сделать вывод: основной способ защиты от социальной инженерии – это обучение сотрудников.

Необходимо знать и помнить, что незнание не освобождает от ответственности. Каждый пользователь системы должен знать об опасности раскрытия конфиденциальной информации и знать способы, которые помогут предотвратить утечку. Предупрежден – значит вооружен!

Список литературы:

1. Касперски К. Секретное оружие социальной инженерии. (Электрон. ресурс) / Способ доступа: URL: http://citforum.ru/security/articles/soc_eng/ – Секретное оружие социальной инженерии;
2. Шишкова С. Социальная инженерия (Электрон. ресурс) / Способ доступа: URL: <http://www.executive.ru/knowledge/announcement/345004/> – Социальная инженерия;
3. Полонская Е. Социальная инженерия: защита от умного, который использует дурака (Электрон. ресурс) / Способ доступа: URL: http://citforum.ru/security/articles/s_engenering/index.shtml/ – Социальная инженерия: защита от умного, который использует дурака.
4. Should Social Engineering be a part of Penetration Testing? (Электрон. ресурс) / Способ доступа: URL: <http://www.darknet.org.uk/2006/03/should-social-engineering-a-part-of-penetration-testing/> – Should Social Engineering be a part of Penetration Testing?

Киреев В.В.

Научный руководитель: Поляруш В.В.

*ПОУПК «Донецкий экономико-правовой кооперативный техникум
имени Н.П. Баллина»*

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Под информационной безопасностью понимается защищённость информации и поддерживающей ее инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или поддерживающей инфраструктуре.

Информационная безопасность организации - состояние защищённости информационной среды организации, обеспечивающее её формирование, использование и развитие [1].

Термин «безопасность информации» описывает ситуацию, исключающую доступ для просмотра, модерации и уничтожения данных субъектами без наличия соответствующих прав. Это понятие включает обеспечение защиты от утечки и кражи информации с помощью современных технологий и инновационных устройств.

Защита информации включает полный комплекс мер по обеспечении целостности и конфиденциальности информации при условии ее доступности для пользователей, имеющих соответствующие права.

Целостность – понятие, определяющее сохранность качества информации и ее свойств.

Конфиденциальность предполагает обеспечение секретности данных и доступа к определённой информации отдельным пользователям.

Доступность – качество информации, определяющее ее быстрое и точное нахождение конкретными пользователями.

Цель защиты информации – минимизация ущерба вследствие нарушения требований целостности, конфиденциальности и доступности [2].

В качестве стандартной модели безопасности часто приводят модель из трёх категорий:

- Конфиденциальность - состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право;
- Целостность - избежание несанкционированной модификации информации;
- Доступность - избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.

Также, надёжная система защиты должна соответствовать следующим принципам:

- Стоимость средств защиты должна быть меньше, чем размеры возможного ущерба.
- Каждый пользователь должен иметь минимальный набор привилегий, необходимый для работы.
- Защита тем более эффективна, чем проще пользователю с ней работать.
- Возможность отключения в экстренных случаях [3].

Под угрозами конфиденциальной информации принято понимать потенциальные или реально возможные действия по отношению к информационным ресурсам, приводящие к неправомерному овладению охраняемыми сведениями.

Таковыми действиями являются:

- Ознакомление с конфиденциальной информацией различными путями и способами без нарушения ее целостности;
- Модификация информации в криминальных целях как частичное или значительное изменение состава и содержания сведений;
- Разрушение (уничтожение) информации как акт вандализма с целью прямого нанесения материального ущерба.

В конечном итоге противоправные действия с информацией приводят к нарушению ее конфиденциальности, полноты, достоверности и доступности, что в свою очередь приводит к нарушению как режима управления, так и его качества в условиях ложной или неполной информации. Каждая угроза влечёт за собой определённый ущерб - моральный или материальный, а защита и противодействие угрозе призвано снизить его величину, в идеале - полностью, реально - значительно или хотя бы частично. Но и это удаётся далеко не всегда.

С учётом этого угрозы могут быть классифицированы по следующим кластерам:

1. по величине принесённого ущерба:
 - предельный, после которого фирма может стать банкротом;
 - значительный, но не приводящий к банкротству;
 - незначительный, который фирма за какое-то время может компенсировать и др.;
2. по вероятности возникновения:
 - весьма вероятная угроза;
 - вероятная угроза;
 - маловероятная угроза;
3. по причинам появления:
 - стихийные бедствия;
 - преднамеренные действия;
4. по характеру нанесённого ущерба:
 - материальный;
 - моральный;
5. по характеру воздействия:
 - активные;
 - пассивные;
6. по отношению к объекту:
 - внутренние;
 - внешние.
7. Источниками внешних угроз являются:
 - недобросовестные конкуренты;
 - преступные группировки и формирования;
 - отдельные лица и организации административно-управленческого аппарата.
8. Источниками внутренних угроз могут быть:
 - администрация предприятия;
 - персонал;
 - технические средства обеспечения производственной и трудовой деятельности.

Соотношение внешних и внутренних угроз на усреднённом уровне можно охарактеризовать так (Рисунок 1).

Вывод: угроза - это потенциальные или реальные действия, приводящие к моральному или материальному ущербу [4].

Сейчас эта гонка вооружения - хакеры ломают то, что придумано разработчиками, а разработчики антивирусов придумывают новые способы и методы защиты и пока это - порочный круг.

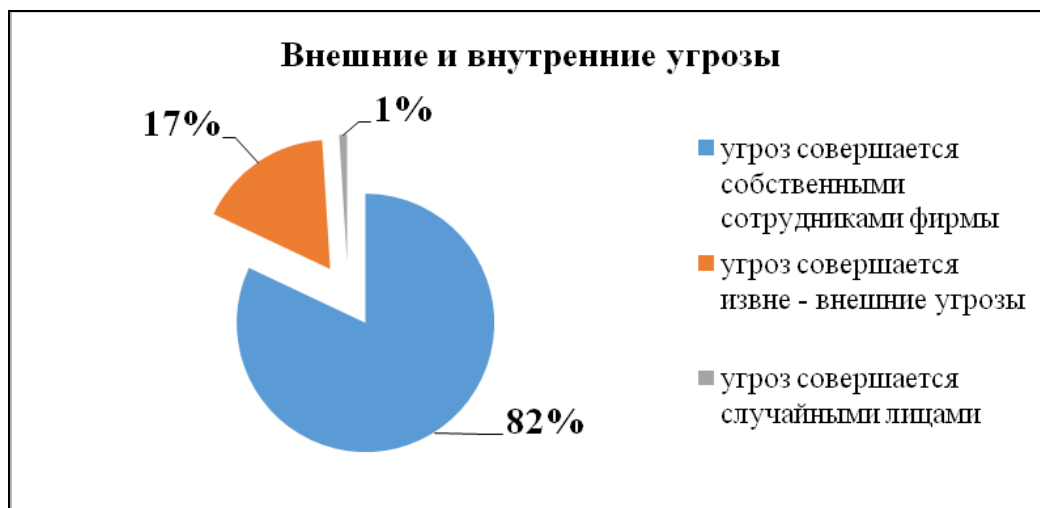


Рисунок 1. Статистика соотношения внешних и внутренних угроз на усреднённом уровне

Список литературы:

1. Информационная безопасность и ее составляющие. - [Электронный ресурс]. – Режим доступа: <https://www.bibliofond.ru/view.aspx?id=783812>
2. Обеспечение информационной безопасности организации. - [Электронный ресурс]. – Режим доступа: <http://www.iccwbo.ru/blog/2016/obespechenie-informatsionnoy-bezopasnosti/>
3. Информационная безопасность. - [Электронный ресурс]. – Режим доступа: <https://works.doklad.ru/view/64ZKFOqS1eI.html>
4. Информационная безопасность. [Электронный ресурс]. – Режим доступа: <http://www.neuch.ru/referat/6889.html>

Куделько Я.А.

Научный руководитель: Давидчук Н.Н, к.э.н., доцент

*ГО ВПО «Донецкий национальный университет экономики и торговли
имени Михаила Туган-Барановского»*

УГРОЗЫ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ СЕТИ КОМПАНИИ

В настоящее время происходит стремительный скачок развития информационной сферы, все больше появляется новой информации и информационных источников для применения в практической деятельности компаний, информационных технологий, которые дают возможность компаниям оптимизировать свою работу за счет цифровых копий данных, все это обеспечивает быстрый доступ к данным, долгосрочное хранение без износа конечного источника информации, сохранение физического пространства, минимизацию затрат на оплату труда, автоматизацию обработки и анализа полученной информации и т.д. [1].

Однако, кроме положительных сторон от развития информации и ее способов использования, существуют и отрицательные моменты в использовании информационной системы компанией[2]:

- Сложность обеспечения информационной безопасности компании;
- Обслуживание необходимых информационных носителей;
- Ноем квалифицированных специалистов в области обеспечения и обслуживания безопасности информационной системы;
- Проведение резервного копирования большого объема информации;
- Разработка или покупка необходимого специфического программного обеспечения для конкретного типа компаний.

Для того чтобы компания была рентабельна и конкурентоспособна, на всех уровнях должен быть доступ к информации, которая необходима для ее деятельности, следовательно, необходима защита информации и действующая система информационной безопасности. Поэтому поднимается вопрос о безопасности и защите корпоративной сети компании, так как через нее проходит все информация о деятельности компании и ее сотрудниках. Остановка и появление преград данного потока информации способна тормозить всю деятельность компании, что может привести к потерям прибыли, получению убытка, кроме этого сбой в корпоративной сети является угрозой потери имиджа или привести к частичной или полной остановке деятельности компании.

Угрозами для информационных технологий и инфраструктуры являются вирусы, такие как черви и троянское ПО; шпионское ПО; спам и фишинг-атаки сети; социальный инжиниринг [3].

Угрозы безопасности корпоративной сети компании являются серьезной проблемой для компании. Получив доступ к корпоративной сети, злоумышленник может воспользоваться конфиденциальной информацией в личных целях или передать ее конкурентам. С помощью определенных манипуляций, злоумышленник доступ получает через один из компьютеров корпоративной сети компании, тем самым имеет прямое подключение к локальной сети компании изнутри, что приводит к сбоям в работе, утечке информации или ее полной потери.

Одной из распространённых угроз безопасности информации является веб-атака, которая заключается в использовании вредоносных URL- адресов для передачи вредоносных программ или вирусные сценарии для взламывания легальных сайтов [4].

Спам-атаки представляют собой массовую рассылку рекламных или коммерческих сообщений, они часто содержат в себе вирусные файлы и программы. Сетевые атаки – это удаленное воздействие на компьютер с использованием различных программ. С помощью сетевых атак можно получить доступ к информации, чужому компьютеру, или же изменить существующие файлы. Такие атаки для получения информации имеют сложный характер в создании и использовании, поэтому случаев сетевых атак небольшое количество, но ущерб от них достаточной большой для компании.

Реализация вирусных программ и алгоритмов является одной из причин остановки информационной системы, утечке данных или подмене файлов с данными. Поэтому главной задачей системы безопасности информации компании является обеспечения конфиденциальности данных и гарантированной защиты информации от несанкционированного воздействия.

Современная система безопасности корпоративной сети должна действовать на следующих принципах [3]:

1. Комплексная защита информации, которая включает в себя использование различных методов и аппаратных программ защиты.
2. Своевременное реагирование на возникшие проблемы.
3. Непрерывность защиты информации, так как поток информации поступает непрерывно по корпоративной сети.
4. Контроль мероприятий по защите информационной системы.

Правильное использование защитных технологий обеспечит максимальную защиту информации в корпоративной сети компании. Кроме традиционных методов защиты информации, существуют методы, которые применяются в различных сферах деятельности, и которые могут быть использованы не хуже или лучше, чем уже имеющиеся методы на рынке [5].

Так вышесказанное свидетельствует о том, что внутренняя информация компании, ее корпоративная сеть, нуждается в проведении защитных механизмов в рамках системы информационной безопасности компании. Это ядро компании, которое обеспечивает непрерывную деятельность компании и ее отделов, а пренебрежение в защите информации и безопасности информационной системы приведет к негативным последствиям касательно операционной деятельности, ее сотрудников, финансов и имиджа компании.

Список литературы:

1. Мазуров В.А., Невинский В.В. Понятие и принципы информационной безопасности / В.А. Мазуров, В.В. Невинский // Известия Алтайского государственного университета: 2003. – с.57-63
2. . Родионов, М. А. Методологические аспекты информационного аудита в менеджменте предприятия / М. А. Родионов. — Научный Вестник МГТУ ГА. — 2009. — № 156. — С. 68–74
3. Карасёв П. А, Столяренко А. В. Информационная безопасность в корпоративных сетях / П.А. Карасёв, А.В. Столяренко // Таврический научный обозреватель. - № 3 (20). – 2017. – с. 208-213.
4. Табилова А.З., Коннов В.Л. Анализ проблем информационной безопасности в корпоративных сетях / А.З. Табилова, В.Л. Коннов // Вестник науки и образования: № 17(71). – 2019. – с.10-12
5. Кубаренко А.С. Модернизация корпоративной компьютерной сети предприятия // Научно-методический электронный журнал «Концепт», 2016. – Т.11. – с.3131–3135. [Электронный ресурс]. Режим доступа: <http://e-koncept.ru/2016/86662.htm/>

МЕТОДЫ АНАЛИЗА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Анализ рисков информационной безопасности становится все более важным компонентом организации предпринимательской деятельности.

Анализ рисков информационной безопасности – это, прежде всего, процесс, входящий в непрерывную процедуру защиты информации. Комплекс мероприятий по оценке состояния защищенности инфраструктуры, в которой осуществляется манипуляция чувствительной для бизнеса информацией.

Традиционный анализ рисков информационной безопасности можно разделить на несколько этапов, в которые входят количественный и качественный. Количественные и качественные методы анализа имеют ряд преимуществ перед другими видами анализа информационных рисков.

Тем не менее, иерархический процесс широко используется в оценке безопасности. Будущее направление исследований может быть разработка и применение мягких вычислений, таких как грубые множества, серые множества, нечеткие системы, общие алгоритмы, метод опорных векторов, байесовская сеть и гибридная модель. Гибридная модель разработана путем интеграции двух или более существующих моделей. Этот подход сочетается с процессом аналитической иерархии и нечетким комплексным методом.

Анализ рисков является основой защиты информации и включает в себя такие процессы, как идентификация деятельности, анализ угрозы, анализ уязвимостей и т.д.

В процессе анализа рисков информационной безопасности выделяются несколько этапов. Основным этапом является проведение комплексного анализа для выявления рисков и их оценки. Качественный и количественный метод оценки рисков информационной безопасности являются основными, используемыми для анализа риска, которому подвергаются активы предприятия. Также наряду с преимуществами присутствуют и недостатки оценки риска информационной безопасности внутри системы (Таб. 1).

Таблица 1 - Преимущества и недостатки количественных и качественных методов оценки рисков

Количественные методы	
Преимущества	– определение последствий, возникновения инцидентов; – проведение анализа затрат и выгод при выборе защиты; – получение более точного изображения риска.
Недостатки	– прямая зависимость количественных мер от объема и точности определяемой шкалы;

	<ul style="list-style-type: none"> – погрешность результатов анализа; – отсутствие обогащения качественным описанием; – высокая стоимость анализа, необходимость в большом опыте и передовых технологиях.
Качественные методы	
Преимущества	<ul style="list-style-type: none"> – определение зон повышенного риска в короткие сроки и без больших затрат; – простота и низкая стоимость анализа.
Недостатки	<ul style="list-style-type: none"> – отсутствие возможности определения вероятности и результатов с использованием численных мер; – усложнение анализа выгод и затрат при выборе средств защиты; – погрешность достигнутых результатов.

Процесс включает в себя подготовку к оценке рисков, идентификацию активов, идентификацию угроз, определение уязвимости процесса идентификации, расчет риска и другие этапы. Процесс может быть разделен на несколько шагов:

- определение объекта оценки: данных информационной системы, аппаратных средств, программного обеспечения, активов, объемов, оценка системы и т.д.;
- оценка эффективности: разработка плана оценки в соответствии с требованиями, выбор соответствующего метода и инструмента оценки и настройка системной группы;
- идентификация риска: определение критических активов, общих активов в рамках оценки. Выявление угроз операционной среды и собственных уязвимостей системы, определение уже существующих мер безопасности;
- анализ рисков: анализ возможности и последствий угрозы, расчёт результатов оценки, анализ эффективности существующих мер;
- оценка риска: оценка результатов; формирование отчета об оценке риска в сочетании с мнением эксперта;
- контроль риска: для эффективного контроля рисков и угроз в соответствии с инструкциями необходимо принять меры для снижения риска;

Процесс оценки риска информационной безопасности является важной предпосылкой для достижения эффективного противостояния рискам. Таким образом, для эффективного выявления угроз и определения рисков необходимо использовать качественный и количественный методы в комплексе тем самым повышая качество прогнозирования рисков и противодействие угрозам.

Список литературы:

1. Депэн Дэн Оценка риска информационной безопасности с помощью машины опорных векторов / Дэн Депэн, Мэн Чжэнь // Журнал Хуажонге университета науки и технологии (естествознание издание). – 2010. – № 3(38). – С. 46-49.

2. Shi, H. Серая модель оценки безопасности информационных систем /H. Shi, Y. Deng // Журнал вычислительной техники. – 2012 – Вып. 7. – № 1. – С. 284-291.

3. Кидзе Н. Анализ конкурентоспособности китайской стали и южнокорейского программного обеспечения вычислительной техники в информационно-коммуникационных технологиях / Н. Кидзе, Дж. Ло // Вып. 2. –2012. – № 1. – С. 451-460.

4. Шукла Н. Сравнительное исследование практики анализа рисков информационной безопасности / Н. Шукла, С.А Кумар // В ходе рассмотрения вопросов и проблем в области сетевого взаимодействия. – 2012. – С. 28-33.

5. Сямсуддин И. Оценка стратегической информационной безопасности с помощью нечеткого метода АНР / И. Сямсуддин // Американский журнал разведывательных систем. – Вып. 2. – № 1. – С. 9-13.

Пенез Р.В.

ГОО ВПО «Донецкая академия внутренних дел Министерства внутренних дел Донецкой Народной Республики», Донецк, ДНР.

ПРЕОДОЛЕНИЕ ПРОТИВОДЕЙСТВИЯ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ПРЕДВАРИТЕЛЬНОГО РАССЛЕДОВАНИЯ КАК ЭЛЕМЕНТ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Противодействие реализации государственно-властных полномочий сотрудниками следствия и дознания при осуществлении уголовного судопроизводства является одним из видов противоправной деятельности, покушающейся на государственную монополию установления законности и соблюдения прав и свобод граждан.

Устоявшееся в науке понимание преодоления противодействия расследованию, как формы и способа сокрытия преступления, претерпело значительные трансформации и в настоящее время все чаще рассматривается как умышленная деятельность. Ее целью является воспрепятствования решению задач расследования и, в конечном счете, установлению истины по уголовному делу. Современная следственная практика свидетельствует о том, что противодействие расследованию оказывает не только обвиняемая сторона, но и потерпевший, и даже свидетель.

Одной из наиболее распространенных форм противодействия расследованию, помимо введения в заблуждение следственные органы, являются попытки физического уничтожения материальных носителей по уголовным делам, протоколов, вещественных доказательств и т.д. Помимо умышленного уничтожения материалов уголовного дела, немаловажную роль играет и человеческий фактор, следствием чего может стать неумышленная утрата или порча материалов уголовного дела: потеря, залитие, сгорание и т.д. В этой связи оцифровка материальных носителей, связанных с уголовным

судопроизводством, раскрывает широкие возможности их воссоздания и копирования, в т. ч. и 3D моделирование.

Проблематика применения информационных технологий при осуществлении уголовного судопроизводства исследовалась такими учеными, как Ю.Н. Соколов, Д.А. Натура, А.А. Сарапулов, И.П. Катеринчук, Л.А. Воскобитова и др. Однако работы указанных авторов посвящались, преимущественно, ведению статистической отчетности и формированию электронного варианта бланков уголовно-процессуальных документов, ведению криминалистических учетов и регистрации. Вместе с тем, применение таких технологий как трехмерное сканирование обстановки и обстоятельств события и вещественных доказательств в уголовном судопроизводстве - практически не разработано. За рубежом рассматриваемой проблеме уделяется усиленное внимание. Так, например, в Казахстане принят закон «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам модернизации процессуальных основ правоохранительной деятельности», который предусматривает возможность ведения уголовного судопроизводства в электронном формате [1]. Стоит отметить, что Казахстаном в рамках модернизации уголовного судопроизводства также была принята инструкция о ведении уголовного дела в электронном формате [2]. Данная инструкция включает в себя порядок формирования и ведения уголовного дела в электронном формате на стадии предварительного расследования. Исходя из этого, можно сделать вывод, что за рубежом заинтересованы во внедрении цифровых инноваций в уголовное судопроизводство, в том числе и ведении уголовного дела в электронном формате.

В связи с этим, нами предлагается создание копии материалов уголовных дел в электронном формате, а также создание трехмерных копий вещественных доказательств, что позволит значительно снизить риск фальсификации материалов уголовного дела – в первую очередь в отношении следственных и процессуальных действий.

Преодоление противодействия деятельности органов предварительного расследования в рамках обеспечения информационной безопасности в ДНР является проблематичными, требует решения ряда законодательных, информационно-технических и материально-технических задач.

Во-первых, решение вопросов законодательного характера, а именно определение субъекта, который будет вести уголовное дело в электронном формате, 3D проектирование вещественных доказательств и осуществлять лазерное сканирование места происшествия. Эту задачу предлагается возложить на следователя, в производстве которого находится данное уголовное дело, и на законодательном уровне закрепить обязанность следователя сканировать и загружать все материалы уголовного дела в информационную базу, производить лазерное сканирование места происшествия и при необходимости осуществлять 3Dкопирование вещественных доказательств. Очевидно, что изготовление оцифрованных материалов уголовного дела, создание 3Dкопий вещественных доказательств и

осуществление лазерного сканирования места происшествия требует затрат определенного времени и наличие специальных знаний, в связи с чем необходимо расширить штат следственных подразделений специалистами, на которых будут возложены вышеуказанные задачи.

Во-вторых, решение информационно-технической стороны путем создания единой электронной базы следственных подразделений с ограниченным доступом, которая вмещала бы в себя архивы с копиями оцифрованных уголовных дел. Доступ к данным будет осуществляться следователем посредством введения индивидуального логина и пароля. Для решения вопросов унификации процессуальной формы электронного документа предлагается также установить формат подачи материалов уголовного дела, например, PDF (или аналогичные ему).

В-третьих, следует решить материально-техническую сторону данного вопроса, увеличив обеспечение следственных подразделений организационной техникой, в частности, сканерами, лазерными сканерами, 3D принтерами.

Необходимость материально-технических и информационно-ресурсных затрат на реализацию вышеуказанных предложений оправдано угрозой активизации на территории ДНР боевых действий, что может повлечь порчу материалов уголовного дела и вещественных доказательств. Кроме того, надежно защищенный цифровой носитель поможет сохранить материалы уголовного дела от утраты, порчи, а также значительно снизить риск фальсификации материалов уголовного дела.

Список литературы:

1. Закон Республики Казахстан от 21 декабря 2017 года № 118-VI «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам модернизации процессуальных основ правоохранительной деятельности» [Электронный ресурс]. – Режим доступа: http://online.zakon.kz/document/?doc_id=35167041#pos=2;-160.

2. Приказ Генерального прокурора Республики Казахстан от 3 января 2018 года № 16268 «Об утверждении Инструкции о ведении уголовного судопроизводства в электронном формате» [Электронный ресурс]. – Режим доступа: <http://adilet.zan.kz/rus/docs/V1800016268>.

Решетько М.А., аспирант
Научный руководитель: Шершнёва А.В., к.э.н., доцент

*ГО ВПО «Донецкий национальный университет экономики и торговли
имени Михаила Туган-Барановского»*

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ НА ПРЕДПРИЯТИИ

С развитием информационных технологий и компьютеризацией экономики важнейшим из вопросов в деятельности предприятия становится обеспечение информационной безопасности.

Информация является наиболее ценным и важным активом предприятия и в свою очередь она должна быть защищена надлежащим образом.

Информационная безопасность – это сохранение и защита информации, а также ее важнейших элементов. Информационная безопасность предприятия в свою очередь это набор необходимых средств, методов и работ которые ориентированы на защиту информационной структуры самого предприятия от внешних или внутренних угроз, которые могут спровоцировать кражу, порчу или изменение данных на серверах или рабочих станциях.

Целью обеспечения информационной безопасности является защита информационных данных и поддержание инфраструктуры предприятия от случайного или специального вмешательства, которое может привести к краже или потере данных. Обеспечение информационной безопасности помогает обеспечить непрерывную работу предприятия и защиту конфиденциальной информации.

Что же может представлять угрозу информационной безопасности? Таких факторов достаточно много. Это и умышленные действия конкурентов или недоброжелателей, что чаще всего встречается на больших предприятиях, так и умышленные или не умышленные действия самих сотрудников, которые могут быть выявлены практически на любом предприятии.

Все эти факторы можно разделить на несколько видов:

1. **Угроза от авторизованных пользователей.** Сюда входят умышленные и не умышленные (в результате халатности) действия сотрудников предприятия, работающих с информационной системой. Такие действия могут приводить к краже, уничтожению или изменению данных на серверах или рабочих станциях без какого-либо постороннего вмешательства в информационную инфраструктуру.

2. **Внешние целенаправленные внешние атаки.** В эту группу входят действия предполагающие не санкционированное проникновение в компьютерную сеть из вне, а так же DDOS атаки. Целью таких атак, зачастую, является уничтожение или кража конфиденциальной информации, изменение алгоритмов работы сетей и оборудования, удаление данных серверов, вмешательство в системы управления бизнес процессами.

3. **Компьютерные вирусы.** Именно это является наиболее опасной для информационной инфраструктуры компании, так как является наиболее распространенной. Источником проникновения вируса может быть электронная почта, интернет, внешние носители информации и т.д. Результатом действия вируса может быть как кража информации (зачастую паролей доступа), так и ее уничтожение.

4. **СПАМ** – это сообщения, зачастую массовая рассылка, приходящие из не санкционированных источников. Сегодня СПАМ обрел такое распространение, что его можно смело отнести к источникам угроз информационной безопасности предприятия. Обилие СПАМа приходящего на почтовые адреса сотрудников предприятия может вызвать потерю важной корреспонденции, которую просто сложно найти в обилии СПАМ сообщений. Так же СПАМ может быть источником проникновения компьютерных вирусов,

зачастую троянов, или просто приводить к перегрузке почтовых серверов или маршрутизаторов.

5. К отдельной группе можно отнести **форс-мажорные обстоятельства**. Такие как порча оборудования в результате износа, не правильного использования или внешних факторов. Такие обстоятельства тоже могут приводить к потере данных, и их тоже необходимо учитывать в процессе проектирования системы информационной безопасности.

На сегодняшний день существует множество способов борьбы с угрозами информационной безопасности. Для каждой угрозы подбираются свои методы и процессы, которые контролируют определенные «узлы» информационной системы и предотвращают какие-либо сбои в них. Однако максимального эффекта можно добиться только применением всех методов в комплексе. Другими словами, проектирование, построение, внедрение и поддержка системы информационной безопасности – это комплексная задача, требующая анализа потенциальных угроз, выбора методов борьбы с ними и налаживания взаимодействия между этими методами.

Основными средствами и методами защиты информации являются:

1. Система аутентификации. Представляет собой основной метод защиты информации практически в любой сфере. Сводится к тому, что для получения доступа к той или иной информационной области, консоли управления или каналу связи пользователю необходимо предоставить системе свои данные аутентификации (зачастую логин и пароль).

2. Система шифрования. Данная система ориентирована на то, что бы злоумышленник, которому удалось, перехватить определенные данные не мог, получить доступ к этим данным не имея определенного ключа. Шифрование данных делится на два вида: шифрование с открытым ключом и шифрование с закрытым ключом.

3. Межсетевой экран. Система межсетевого экрана или брандмауэра ставит своей целью отделение локальной сети конкретного предприятия от глобальной сети Интернет.

4. VPN (виртуальные частные сети). Данная технология позволяет передавать данные через глобальные общедоступные сети, такие как Интернет, через безопасные зашифрованные VPN тоннели. Таким образом, информация хоть и передается через глобальную сеть, однако не может быть доступна из нее несанкционированно.

5. Фильтрация электронной почты. Эта система позволяет устанавливать определенные фильтры на содержимое входящей и исходящей корреспонденции. Таким образом оберегает внутреннюю сеть от проникновения нежелательных данных, в частности вирусов, а так же исключая утечку определенных видов информации из внутренней сети.

6. Антивирусная защита. Ориентирована на предотвращение угроз со стороны компьютерных вирусов. Тесно взаимосвязана с фильтрацией электронной почты и межсетевым экраном.

7. Использование систем выявления слабых мест. Способствует выявлению слабых мест в системе защиты информации путем моделирования

действий злоумышленника и тестирования работы системы при таких действиях.

Рогожников А.С.

ГОО ВПО «Донецкая академия внутренних дел МВД ДНР»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

В современном обществе информация является одним из важнейших стратегических и управленческих ресурсов. Ее производство и потребление составляют необходимую основу эффективного функционирования и развития различных сфер общественной жизни, и, прежде всего, экономики. Именно поэтому информационная безопасность является одной из глобальных проблем современности.

Большая часть интересов любого субъекта хозяйственной деятельности определяется состоянием окружающей информационной среды. Целенаправленные или непреднамеренные действия со стороны внешних или внутренних источников могут задать вред этим интересам и представляют реальную угрозу для дальнейшей деятельности субъекта. Все больше руководителей понимают, насколько опасной может быть инсайдерская информация, системы обработки информации и действия сотрудников, участвующих в деятельности предприятия.

К наиболее распространенным видам потенциальных угроз безопасности предприятия в сфере информационных технологий относят:

- нерегламентированный доступ к файлам данных;
- свободное вмешательство в программное обеспечение;
- отсутствие протоколирования изменений в программном обеспечении;
- отсутствие регламентации пользователей информации;
- отсутствие схем информационного обеспечения уровней управления;
- наличие неподотчетных должностных лиц в системе управления.

Создавая системы безопасности на предприятии, необходимо учитывать, что для эффективной защиты информационных ресурсов требуется реализация целого ряда разнообразных мероприятий, которые можно разделить на три группы: юридические, организационно-экономические и технологические. Хотя разработкой мероприятий в каждой из трех групп должны заниматься специалисты соответствующих отраслей знаний, применяющих свои способы и методы для достижения заданных целей, успех в значительной мере будет зависеть от того, насколько в рамках системного подхода удастся определить и реализовать взаимные связи между соответствующими определениями, принципами, способами и механизмами защиты.

В современном представлении ролевых функций службы информационной безопасности можно выделить четыре направления:

1) разработка методологии и методик анализа угроз, оценки уровня информационной безопасности предприятия и системы ее обеспечения;

2) организация и осуществление конкретных видов деятельности по защите информации;

3) эксплуатация технических средств защиты информации;

4) аудит и контроль функционирования системы информационной безопасности предприятия.

Задачу обеспечения информационной безопасности необходимо решать системно. Это означает, что средства защиты информации должны применяться одновременно и под централизованным управлением. При этом компоненты системы должны «знать» о существовании друг друга, взаимодействовать и обеспечивать защиту от внешних и от внутренних угроз.

Технологии защиты данных основываются на применении современных методов, которые предотвращают утечки информации и ее потерю. Сегодня используется шесть основных способов защиты: препятствие, маскировка, регламентация, управление, принуждение, побуждение.

Все перечисленные методы нацелены на построение эффективной технологии защиты информации.

Под препятствием понимается способ физической защиты информационных систем, благодаря которому злоумышленники не имеют возможности попасть на охраняемую территорию.

Маскировка – способ защиты информации, предусматривающий преобразование данных в форму, непригодную для восприятия посторонними лицами. Для расшифровки требуется знание принципа.

Управление – способ защиты информации, при котором осуществляется управление над всеми компонентами информационной системы.

Регламентация – важнейший метод защиты информационных систем, предполагающий введение особых инструкций, согласно которым должны осуществляться все манипуляции сохраняемыми данными.

Принуждение – метод защиты информации, тесно связанный с регламентацией, предполагающий введение комплекса мер, при котором работники вынуждены выполнять установленные правила.

Когда используются способы воздействия на работников, то речь идет о побуждении.

Способы защиты информации предполагают использование определенного набора средств. Для предотвращения потери и утечки секретных данных используются средства:

- физические;
- аппаратные;
- программные;
- аппаратно-программные;
- законодательные;
- криптографические и организационные методы.

Физические средства защиты – это средства, необходимые для внешней защиты средств вычислительной техники, территории и объектов.

Аппаратные средства защиты – это различные электронные, электронно-механические и другие устройства, которые монтируются в серийные блоки электронных систем обработки и передачи данных для внутренней защиты средств вычислительной техники: терминалов, устройств ввода и вывода данных, процессоров, линий связи и т.п.

Программные средства защиты, встроенные в состав программного обеспечения системы, необходимы для выполнения логических и интеллектуальных функций защиты.

Аппаратно-программные средства защиты – это средства, основанные на синтезе программных и аппаратных средств.

Законодательные средства – комплекс нормативно-правовых актов, регулирующих деятельность людей, имеющих доступ к охраняемым сведениям и определяющих меру ответственности за потерю или кражу секретной информации.

Организационные меры защиты информации составляют совокупность мероприятий по подбору, проверке и обучению персонала, участвующего во всех стадиях информационного процесса.

Итак, в современных условиях информационная безопасность является неотъемлемой составляющей системы экономической безопасности хозяйствующего субъекта. В свою очередь, надежное обеспечение информационной безопасности является неременным условием перехода на модель устойчивого развития не только отдельного предприятия, но и национальной экономики в целом. Чтобы сохранить бизнес, развиваться и быть конкурентоспособным, предприятиям необходимо создать эффективную систему управления информационной безопасностью. Сущность изложенного дает основания утверждать, что в современных условиях, без должной защиты информационной среды предприятия, невозможно обеспечить его экономическую безопасность.

Список литературы:

1. Белов Е. Б., Лось В. П. Основы информационной безопасности. М.: Горячая линия: Телеком, 2006.
2. Мельников В. П., Клейменов С. А., Петраков А. М. Информационная безопасность и защита информации. 3-е изд. М.: Академия, 2008.
3. Расторгуев С. П. Основы информационной безопасности: учебное пособие / С. П. Расторгуев. – М.: Издательский центр "Академия", 2009. – 192 с.
4. Садердинов А.А. Информационная безопасность предприятия: учебное пособие / А.А. Садердинов, В.А. Трайнев, А.А. Федулов. – М.: Дашков и К, 2005.

Самофалова Е.А.
Научный руководитель: Лутай А.П., к.э.н., доцент

*ГО ВПО «Донецкий национальный университет экономики и торговли
имени Михаила Туган-Барановского»*

ПРОБЛЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЩЕСТВА

Информационная безопасность является одной из проблем, с которой столкнулось современное общество в процессе массового использования автоматизированных средств ее обработки.

В данной работе рассмотрим проблему информационной безопасности общества. И основные понятия информационной безопасности, защиты информации.

Проблема информационной безопасности обусловлена возрастающей ролью информации в общественной жизни. Современное общество все более приобретает черты информационного общества.

Информационная безопасность – это свойство сетей связи общего пользования противостоять возможности реализации нарушителем угрозы информационной безопасности.

Информационная безопасность – свойство сетей связи общего пользования сохранять неизменными характеристики информационной безопасности в условиях возможных воздействий нарушителя.

Необходимо иметь в виду, что при рассмотрении проблемы информационной безопасности нарушитель необязательно является злоумышленником. Нарушителем информационной безопасности может быть сотрудник, нарушивший режим информационной безопасности или внешняя среда, например, высокая температура, может привести к сбоям в работе технических средств хранения информации и т. д.

Информационная безопасность – это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации.

Рассматривая информацию как товар можно сказать, что нанесение ущерба информации в целом приводит к материальным затратам. Например, раскрытие технологии изготовления оригинального продукта приведет к появлению аналогичного продукта, но от другого производителя, и, как следствие, владелец технологии, а может быть и автор, потеряют часть рынка и т. д.

С другой стороны, рассматривая информацию как субъект управления (технология производства, расписание движения транспорта и т. д.), можно утверждать, что изменение ее может привести к катастрофическим последствиям в объекте управления – производстве, транспорте и др.

Именно поэтому при определении понятия "информационная безопасность" на первое место ставится защита информации от различных воздействий.

Поэтому под защитой информации понимается комплекс мероприятий, направленных на обеспечение информационной безопасности.

Защита информации - это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Решение проблемы информационной безопасности, как правило, начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем. Это обусловлено тем, что для разных категорий субъектов характер решаемых задач может существенно различаться.

Например, задачи решаемые администратором локальной сети по обеспечению информационной безопасности, в значительной степени отличаются от задач, решаемых пользователем на домашнем компьютере, не связанном сетью.

При анализе проблематики, связанной с информационной безопасностью, необходимо учитывать специфику данного аспекта безопасности, состоящую в том, что информационная безопасность есть составная часть информационных технологий – области, развивающейся беспрецедентно высокими темпами.

В области информационной безопасности важны не столько отдельные решения (законы, учебные курсы, программно-технические изделия), находящиеся на современном уровне, сколько механизмы генерации новых решений, позволяющие, как минимум, адекватно реагировать на угрозы информационной безопасности или предвидеть новые угрозы и уметь им противостоять.

В ряде случаев понятие "информационная безопасность" подменяется термином "компьютерная безопасность". В этом случае информационная безопасность рассматривается очень узко, поскольку компьютеры только одна из составляющих информационных систем.

Согласно определению, компьютерная безопасность зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электроснабжения, жизнеобеспечения, вентиляции, средства коммуникаций, а также обслуживающий персонал.

Исходя из этого, отметим следующие важные выводы:

- задачи по обеспечению информационной безопасности для разных категорий субъектов могут существенно различаться;
- информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации – это принципиально более широкое понятие.

Ткаченко И.А.
Научный руководитель: Лутай А.П., к.э.н., доцент

*ГО ВПО «Донецкий национальный университет экономики и торговли
имени Михаила Туган-Барановского»*

ЗАДАЧИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЩЕСТВА

Анализ основ информационной безопасности показал, что обеспечение безопасности является задачей комплексной. С одной стороны режима информационной, информационная безопасность предполагает, как минимум, обеспечение трех ее составляющих - доступность, целостность и конфиденциальность данных. И уже с учетом этого проблему информационной безопасности следует рассматривать комплексно. С другой стороны, информацией и информационными системами в буквальном смысле "пронизаны" все сферы общественной деятельности и влияние информации на общество все нарастает, поэтому обеспечение информационной безопасности также требует комплексного подхода.

В этой связи вполне закономерным является рассмотрение проблемы обеспечения информационной безопасности на нескольких уровнях, которые в совокупности обеспечивали бы защиту информации и информационных систем от вредных воздействий, наносящих ущерб субъектам информационных отношений.

В данной работе рассмотрим задачи информационной безопасности общества и выделим три уровня формирования режима информационной безопасности.

Рассматривая проблему информационной безопасности в широком смысле, можно отметить, что в этом случае речь идет об информационной безопасности всего общества и его жизнедеятельности, при этом на информационную безопасность возлагается задача по минимизации всех отрицательных последствий от всеобщей информатизации и содействия развитию всего общества при использовании информации как ресурса его развития.

В этой связи основными задачами информационной безопасности в широком смысле являются:

- защита государственной тайны, т. е. секретной и другой конфиденциальной информации, являющейся собственностью государства, от всех видов несанкционированного доступа, манипулирования и уничтожения;
- защита прав граждан на владение, распоряжение и управление принадлежащей им информацией;
- защита прав предпринимателей при осуществлении ими коммерческой деятельности;
- защита конституционных прав граждан на тайну переписки, переговоров, личную тайну.

Рассматривая проблему информационной безопасности в узком смысле, отметим, что в этом случае речь идет о совокупности методов и средств защиты информации и ее материальных носителей, направленных на обеспечение целостности, конфиденциальности и доступности информации.

Исходя из этого, выделим следующие задачи информационной безопасности:

- защита технических и программных средств информатизации от ошибочных действий персонала и техногенных воздействий, а также стихийных бедствий;
- защита технических и программных средств информатизации от преднамеренных воздействий.

Заметим, что понятие "компьютерная безопасность", как раз подходит под определение информационной безопасности в узком смысле, но не является полным ее содержанием, поскольку информационные системы и материальные носители информации связаны не только с компьютерами.

С учетом изложенного выделим три уровня формирования режима информационной безопасности:

- законодательно-правовой;
- административный (организационный);
- программно-технический.

Законодательно-правовой уровень включает комплекс законодательных и иных правовых актов, устанавливающих правовой статус субъектов информационных отношений, субъектов и объектов защиты, методы, формы и способы защиты, их правовой статус. Кроме того, к этому уровню относятся стандарты и спецификации в области информационной безопасности.

Система законодательных актов и разработанных на их базе нормативных и организационно-распорядительных документов должна обеспечивать организацию эффективного надзора за их исполнением со стороны правоохранительных органов и реализацию мер судебной защиты и ответственности субъектов информационных отношений.

К этому уровню можно отнести и морально-этические нормы поведения, которые сложились традиционно или складываются по мере распространения вычислительных средств в обществе. Морально-этические нормы могут быть регламентированными в законодательном порядке, т. е. в виде свода правил и предписаний.

Административный уровень включает комплекс взаимокоординируемых мероприятий и технических мер, реализующих практические механизмы защиты в процессе создания и эксплуатации систем защиты информации. Организационный уровень должен охватывать все структурные элементы систем обработки данных на всех этапах их жизненного цикла: строительство помещений, проектирование системы, монтаж и наладка оборудования, испытания и проверки, эксплуатация.

Программно-технический уровень включает три подуровня: физический, технический (аппаратный) и программный. Физический подуровень решает

задачи с ограничением физического доступа к информации и информационным системам, соответственно к нему относятся технические средства, реализуемые в виде автономных устройств и систем, не связанных с обработкой, хранением и передачей информации: система охранной сигнализации, система наблюдения, средства физического воспрепятствования доступу (замки, ограждения, решетки и т. д.).

Средства защиты аппаратного и программного подуровней непосредственно связаны с системой обработки информации. Эти средства либо встроены в аппаратные средства обработки, либо сопряжены с ними по стандартному интерфейсу. К аппаратным средствам относятся схемы контроля информации по четности, схемы доступа по ключу и т. д. К программным средствам защиты, образующим программный подуровень, относятся специальное программное обеспечение, используемое для защиты информации, например антивирусный пакет и т. д. Программы защиты могут быть как отдельные, так и встроенные. Так, шифрование данных можно выполнить встроенной в операционную систему файловой шифрующей системой EFS или специальной программой шифрования.

Итак, формирование режима информационной безопасности является сложной системной задачей, решение которой в разных странах отличается по содержанию и зависит от таких факторов, как научный потенциал страны, степень внедрения средств информатизации в жизнь общества и экономику, развитие производственной базы, общей культуры общества и, наконец, традиций и норм поведения.

Тлустый А.О.
Научный руководитель: Хмиленко М.Г.

Торезский колледж Государственного образовательного учреждения высшего профессионального образования «Донецкая академия управления и государственной службы при Главе Донецкой Народной Республики»

ПУТИ РЕШЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Понятие информационная безопасность, имеет длинную историю. С течением времени данный термин не терял своего смысла. В период активного развития компьютерных технологий, информационная безопасность начала приобретать особое значение. А в дальнейшем и вовсе, стала профессией. Так что же представляет собой информационная безопасность?

Информационная безопасность – подразумевает под собой различные способы защиты какой-либо информации. Свое начало информационная безопасность берет в период активного развития локальных сетей, а с началом использование мобильных устройств, угрозы безопасности вовсе выходят на новый уровень. Именно в этот период начинается разработка новых способов

обеспечения безопасности, причиной этому также послужило использование беспроводных сетей для хранения и передачи информации. С активным появлением различных “дыр” в безопасности, возникло сообщество людей, которых называют хакерами. Хакер - человек, который занимается цифровым взломом, крадет, удаляет или подменяет данные, выводит оборудование из строя. Словом, осуществляет несанкционированный доступ к цифровой информации и электронным системам. Хакеры наносят вред в разных объемах, от простых пользователей до крупных корпораций или даже стран. Поэтому вопрос об информационной безопасности становится более насущным, а угрозы, которые представляют хакеры, выходят на государственный уровень[2].

Основная проблема информационной безопасности заключается в том, что она является составной частью информационных технологий. Программирование, к сожалению, не позволяет создавать программы без каких-либо ошибок, либо уязвимостей. Поэтому существует необходимость, создавать системы информационной безопасности с использованием исключительно надежных программ. Но такая необходимость, как ни странно, требует контроля защищенности и соблюдения архитектурных принципов при использовании информационных систем [4].

Но большой проблемой информационной безопасности является обнаружение новых уязвимых мест в программном коде, несмотря на то, что разработчики в кратчайшие сроки стараются устранить такого рода проблемы, это не останавливает злоумышленников, так как они, в свою очередь, активно пользуются данными уязвимостями и, к сожалению, могут нанести огромный вред многим пользователям, включая самих разработчиков [1].

Для защиты информации в информационных системах используют следующие методы:

1) Препятствие – является каким-либо преграждением пути к информации.

2) Управление доступом – представляет собой методы защиты информации через регулирование использования ресурсов информационных технологии и информационной системы. Данный метод должен препятствовать всем возможным путям несанкционированного доступа к защищенной информации. Сам процесс происходит с помощью идентификации пользователей и администратора, а также проверка действующих полномочий доступа к информации, а также метод управления доступом предполагает реагирование, которое выражается в сигнализации, отключении либо отказа в запросе, при попытке несанкционированных действий.

3) Методы криптографии – один из популярных методов защиты информации, заключается в шифровании данных при их обработке и хранении.

Особенно надежным шифрование является при передаче информации по сети, также отличным достоинством метода шифрования является постоянное обновление его алгоритма, что позволяет усложнить попытку атаки при использовании злоумышленниками каких-либо способов расшифровки данных.

4) Регламентация – представляет собой ограничение во времени работы, другими словами данный метод ограничивает доступ людей к информации, причем это ограничение происходит по определенным дням, времени суток, часам. Обеспечение таких условий работы с информацией, нормы и стандарты по защите будут действовать в наибольшей степени.

5) Принуждение – метод защиты, который подразумевает собой какую-либо ответственность за несоблюдение правил работы с защищаемой информацией.

6) Побуждение – метод, который побуждает, за счет соблюдения определенных правил, субъектов информационной системы не нарушать провозглашенные правила [5].

Помимо хакерских атак на веб сайты приходится и доля на атаки конкретных пользователей. Для их защиты существуют следующие средства защиты:

1) Технические средства защиты информации, которые в свою очередь делятся на аппаратные и физические. К аппаратным средствам относятся специальные устройства, которые встраиваются непосредственно в техническое оборудование информационных систем или связываются с ним по интерфейсу. К физическим средствам относят инженерные устройства и сооружения, которые различными способами препятствуют физическому проникновению на защищаемые объекты, и осуществляют защиту материальных, информационных и других ценностей.

2) Программные средства, которые предназначены для защиты информации непосредственно в информационных системах. К ним могут относиться программы для генерации паролей, антивирусные пакеты, программы ограничения доступа и различные программы шифрования.

3) Организационные средства, обеспечивают мероприятия, которые пытаются сделать невозможным или затрудняют разглашение, утечку, несанкционированный доступ к информации на нормативно-правовой основе.

4) Законодательные средства защиты, регламентируют правила работы с информацией и устанавливают порядок ответственности за их нарушение. Данные средства защиты определяются законодательными актами стран.

5) Морально-этические средства защиты, включают нормы поведения, которые, по большей части не утверждены законодательством, но считаются обязательным к исполнению, примером может послужить свод этических правил общения в сети и т.п. [3]

В заключение хочу отметить, что, несмотря на внушительный список методов защиты информации в информационных системах, проблема остается актуальной. Информационная безопасность, несмотря на стремительный рост компьютерных технологий, требует создания новых алгоритмов защиты и внедрения их во все сферы общества.

Список литературы:

1. Шаньгин В.С. Информационная безопасность и защита информации / В.С. Шаньгин.– М.: Пресс, 2017 – 702 с. (дата обращения 05.05.2020).

2. Статья об информационной безопасности. – URL: <http://serachinform.ru/informatsionnaya-bezopasnost/> (дата обращения 05.05.2020).

3. Блог об информационной безопасности. – URL: <http://pirit.biz/resheniya/informacionnaya-bezopasnost> (дата обращения 06.05.2020).

4. Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности / Ю. А. Родичев. – СПб.: Питер, 2017 – 256 с. (дата обращения 07.05.2020).

5. Баранова Е.К. Информационная безопасность и защита информации / Е.И. Баранова, А.А. Бабаш.– М.: Инфра-М, 2016 – 332 с. (дата обращения 08.05.2020).

Халявка А.Г.

Научный руководитель: Хмиленко М.Г.

Торезский колледж Государственного образовательного учреждения высшего профессионального образования «Донецкая академия управления и государственной службы при Главе Донецкой Народной Республики»

КОМПЛЕКСНЫЙ ПОДХОД К ЗАЩИТЕ БИЗНЕС-ИНФОРМАЦИИ

Информация очень важна для успешного развития бизнеса, следовательно, нуждается в соответствующей защите. Особенно актуально это стало в бизнес-среде, где на передний план вышли информационные технологии. Так как мы живем в эпоху цифровой экономики, без них рост компании просто невозможен.

Хрестоматийным стал рассказ о том, как сыновья Ротшильда сделали целое состояние на поражении Наполеона при Ватерлоо 18 июня 1815 года. В начале сражения преимущество находилось на стороне Наполеона, и наблюдатели сообщили в Лондон, что он выигрывает. А курьер Натана Ротшильда Ротворд наблюдал за сражением и видел, как Наполеон бежал в Брюссель и сообщил Натану об этом. Все были убеждены, что Веллингтон проиграл сражение. Тогда Ротшильд немедленно начал продавать на бирже свои облигации. Вслед за ним все стали продавать. В результате цены бумаг упали почти до нуля. В этот момент агенты Ротшильда скупили акции по дешевке. 21 июня в 11 часов вечера адъютант Веллингтона майор Генри Перси доставил в правительство рапорт маршала: «Наполеон разбит».

Таким образом, Натан Ротшильд заработал на этой новости 40 миллионов фунтов стерлингов. Реальная информация, полученная раньше других, позволила Ротшильдам вести беспроигрышную игру на бирже. Именно тогда Натан Ротшильд произносит свой легендарный афоризм: «Кто владеет информацией — тот владеет миром».

А сейчас информация подвергается ещё большему числу угроз и уязвимостей. Хакерские атаки, перехват данных по сети, воздействие вирусных программ и прочие угрозы приобретают более изощренный характер и

набирают огромный темп. Отсюда возникает необходимость внедрять системы информационной безопасности, которые могли бы защитить данные компании.

На выбор подходящих средств защиты информации влияют многие факторы, включая сферу деятельности компании, ее размер, техническую сторону, а также знания сотрудников в области информационной безопасности.

Цель обеспечения информационной безопасности – защитить информационные данные и поддерживающую инфраструктуру от случайного или преднамеренного вмешательства, что может стать причиной потери данных или их несанкционированного изменения. Информационная безопасность помогает обеспечить непрерывность бизнеса. Задачи информационной безопасности сводятся к минимизации ущерба, а также к прогнозированию и предотвращению таких воздействий.

Для того чтобы разобраться в проблеме защиты информации ответим на три вопроса:

- Какую информацию нам необходимо защищать?
- От кого и чего нам необходимо её защищать?
- Каким образом нам необходимо осуществлять защиту информации?

Важно понять, что предприятие должно оберегать далеко не всю информацию, которой оно владеет, а лишь ту, использование которой третьими лицами может нанести ущерб деятельности компании. Напротив, существует и такая информация, которую компании просто необходимо разглашать. Так, нет никакого смысла оберегать от конкурентов информацию о ценах. А вот информацию о ценах и условиях, на которых приобретается продукция, сырьё и материалы необходимо хранить в тайне от конкурентов. Излишняя закрытость компании может стать причиной негативного отношения к ней со стороны потенциальных партнёров, клиентов и инвесторов.

Для успешного внедрения систем информационной безопасности на предприятии необходимо придерживаться трех главных принципов:

1. Конфиденциальность.
2. Целостность.
3. Доступность.

Нужно понимать, что лишь системный и комплексный подход к защите может обеспечить информационную безопасность. В системе информационной безопасности нужно учитывать все актуальные и вероятные угрозы и уязвимости. Для этого необходим непрерывный контроль в реальном времени.

Выбор и внедрение подходящих видов контроля безопасности поможет организации снизить риск до приемлемых уровней. Выделяют следующие виды контроля:

- административный;
- логический;
- физический.

Угрозы информационной безопасности можно разделить на следующие:

- естественные (катаклизмы, независящие от человека: пожары, ураганы, наводнение, удары молнии и т.д.);

- искусственные, которые также делятся на непреднамеренные (совершаются людьми по неосторожности или незнанию) и преднамеренные (хакерские атаки, противоправные действия конкурентов, месть сотрудников и пр.);

- внутренние (источники угрозы, которые находятся внутри системы);

- внешние (источники угроз за пределами системы).

Так как угрозы могут по-разному воздействовать на информационную систему, их делят на пассивные и активные.

Наиболее опасны преднамеренные угрозы, которые все чаще пополняются новыми разновидностями, что связано, в первую очередь, с компьютеризацией экономики и распространением электронных транзакций. Злоумышленники не стоят на месте, а ищут новые пути получить конфиденциальные данные и нанести потери компании.

Чтобы обезопасить компанию от потери денежных средств и интеллектуальной собственности, необходимо уделять больше внимания информационной безопасности. Это возможно благодаря средствам защиты информации с привлечением передовых технологий.

В связи со стремительным развитием информационных технологий, все более частыми кибератаками, компьютерными вирусами и другими появляющимися угрозами, наиболее распространенными и востребованными сегодня являются программные средства защиты информации:

- антивирусные программы;
- облачный антивирус;
- DLP (Data Leak Prevention);
- криптографические системы;
- межсетевые экраны (брандмауэры или файрволы);
- VPN (Virtual Private Network);
- Proxy-server (Прокси-сервер);
- системы мониторинга и управления информационной безопасностью, SIEM.

Отдельное внимание стоит уделять управлению мобильными устройствами на предприятии, так как многие сотрудники часто используют личные смартфоны, планшеты и ноутбуки в корпоративных целях. Внедрение специальных решений, таких как VMware AirWatch, IBM MaaS360, BlackBerry Enterprise Mobility Suite, VMware Workspace One помогут лучше контролировать мобильные устройства сотрудников и защитить данные компании.

Комплексный подход, позволяющий объединить организационные, программные и технические средства защиты информации является одной из актуальнейших задач любой компании, желающей добиться успеха и прибыли в бизнесе.

Список литературы:

1. Родичев Ю.А. Нормативная база и стандарты в области

информационной безопасности / Ю. А. Родичев. – СПб.: Питер, 2017 – 256 с. (дата обращения 07.05.2020).

2. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. / А.Ю.Щербаков - М.: Книжный мир, 2009. – 352 с. (дата обращения 07.05.2020).

3. <https://cyberleninka.ru/article/n/kiberbezopasnost-kak-faktor-razvitiya-tsifrovoy-ekonomiki> (дата обращения 05.05.2020).