УДК: 004.056.53

Карасёв П. А.
обучающийся III курса
направления подготовки 38.03.02 «Менеджмент»
Крымский федеральный университет им. В. И. Вернадского

Научный руководитель: Столяренко А. В.
к.э.н., доцент
кафедры менеджмента и туристского бизнеса
Крымского федерального университета им. В. И. Вернадского

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КОРПОРАТИВНЫХ СЕТЯХ

Статья посвящена актуальной на сегодняшний день проблеме информационной безопасности в корпоративных сетях. В данной статье рассмотрены проблемы защиты конфиденциальной информации в Российской Федерации и способы её сохранения в рамках корпоративных сетей организации. Были изучены причины нарушения безопасности в корпоративной среде и актуальные способы их устранения и усложнения получения доступа к конфиденциальной информации организации, такие как: институциональные методы, антивирусное программное обеспечение (ПО), межсетевые экраны, системы обнаружения атак и VPN. Выявлены основные вирусные угрозы, имеющие наибольшую степень влияния на работу корпоративных сетей и несущие потенциальную угрозу потере или копировании конфиденциальных корпоративных данных или влияние вредоносного программного обеспечения на человеческий ресурс организации с целью манипуляции или хэдхантинга (headhanting). Так же были предложена к рассмотрению альтернативная методика борьбы с угрозами, которая представлена технологией, используемой в сфере медиа контента — DENUVO.

Ключевые слова: *корпоративные сети, безопасность информации, технология.*

Цель — рассмотрение эффективных методов защиты информации в рамках корпоративных сетей.

С каждым годом информационные технологии продолжают стремительно развиваться, тем самым создавая новые способы воздействия на информацию. Развитие информационных технологий дает возможность предприятиям оптимизировать собственную работу за счет цифровых копий данных, которые имеют свой ряд преимуществ перед физическим носителем: быстрый доступ, долгосрочное хранение без износа конечного информационного источника, сохранение физического пространства и т. д. Но помимо положительных моментов присутствует и отрицательный вектор при применении информационных систем: сложность обеспечения безопасности информации, обслуживание информационных носителей, резервное копирование данных и наем специалистов в области обслуживания и безопасности цифровой информации, покупка или разработка специфического программного обеспечения.

Для осуществления эффективного менеджмента в современных реалиях, защита информации, является обязательным условием, так как необходима на всех этапах развития организации. В данном случае мы рассмотрим непосредственно корпоративные сети. Именно они чаще остальных подвергаются угрозам, так как через них идет поток информации характеризующий деятельность организации. Остановка данного потока информации парализует всю деятельность организации, что становится причиной серьезных материальных убытков и потерей имиджа.

Современная информационная безопасность компании базируется на концепции комплексной защиты информации, подразумевающей одновременное использование многих

взаимосвязанных программно-аппаратных решений и мер социального характера, которые поддерживают и дополняют друг друга. Стоит отметить, что помимо традиционных методов защиты, на общем рынке безопасности информации, имеются методы, применяемые в других сферах деятельности, которые могут быть не хуже или лучше, чем те, что уже есть на рынке. Правильное применение данных технологий обеспечит максимально возможную защиту информации в корпоративных сетях любой организации. Таким образом, всё выше описанное подтверждает, то, что информационная безопасть требует особого внимания. Это ядро, которое обеспечивает корректую деятельность всего предприятия и принебрежения ей ведет к негативным финансовым и имеджевым последствиям.

Специалисты отмечают, что главной угрозой для информационных технологий — инфраструктуры являются вирус (троянское ПО, черви), но не стоит забывать, что существенный вред несут и шпионское ПО, спам, фишинг-атаки (вид интернет мошенничества, целью которого является получение доступа к конфиденциальной информации), социальный инжиниринг. По данным АО «Лаборатория Касперского» — международной компании занимающейся разработкой решений для обеспечения информационных технологий — безопасности, мы выводим следующие показатели активных вирусных атак в РФ за последний месяц. Угрозы безопасности локальных вычислительных сетей, являются серьезной проблемой для предприятня, так как это значит, что злоумышленик проник на территорию организации или же завербовал одного из сотрудников. Доступ получает от одного из компьютеров предприятия, тоесть имеет прямое подключение к локальной компьютерной системе компании изнутри, что может привести к массовым сбоям, утечке информации и полной её утере. Ниже приведен график подобных угроз за последний месяц в Российской Федерации (РФ) (рисунке 1).

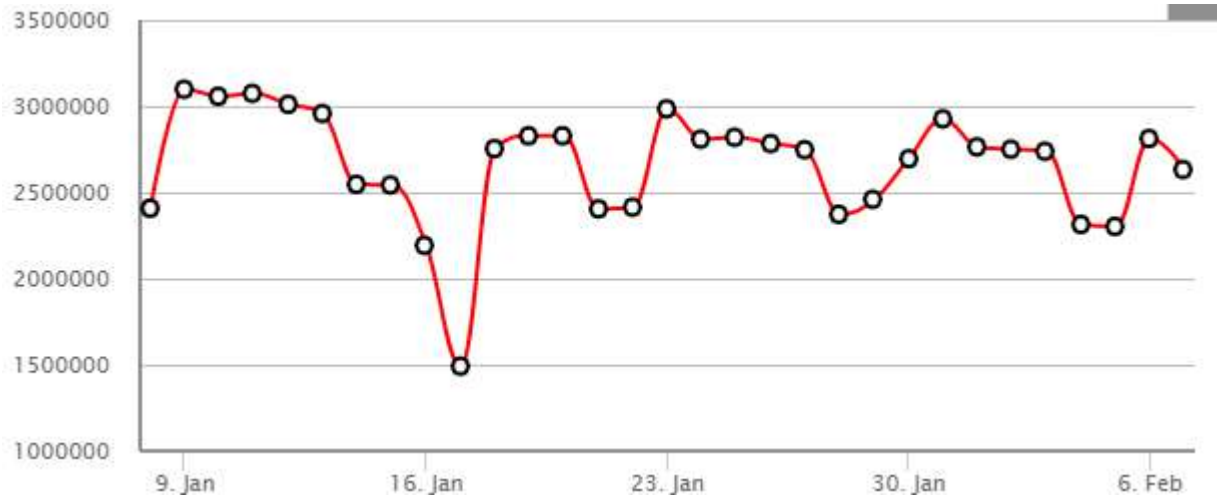

Рисунок 1. — Показатель активных локальных угроз в Российской Федерации за месяц

Веб угрозы — это один из самых распространённых типов атак. Её суть заключается в использовании вредоносных URL- адресов для внедрения вредоносных программ. Так же используют Вредоносные сценарии взламывая легальные сайты. Ниже приведен график активности таких угроз за месяц (рисунке 2).

Далее рассмотрим спам-атаки. Такого рода угрозы — это массовая рассылка сообщений, обычно коммерческого или рекламного характера, часто содержащая вирусные файлы. В корпоративной среде так же может стать предметом угрозы хэдхантинга (headhanting). Активность спам атак за месяц можно отследить по графику предоставленному «Лабораторией Касперского» (рисунок 3).

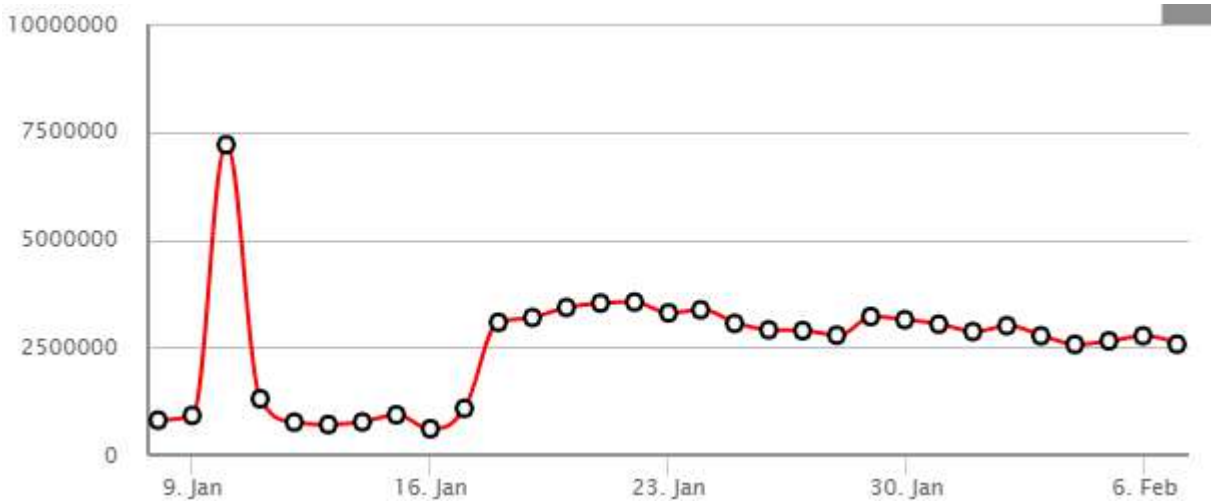

Рисунок 2. — Показатель активных веб угроз в Российской Федерации за месяц

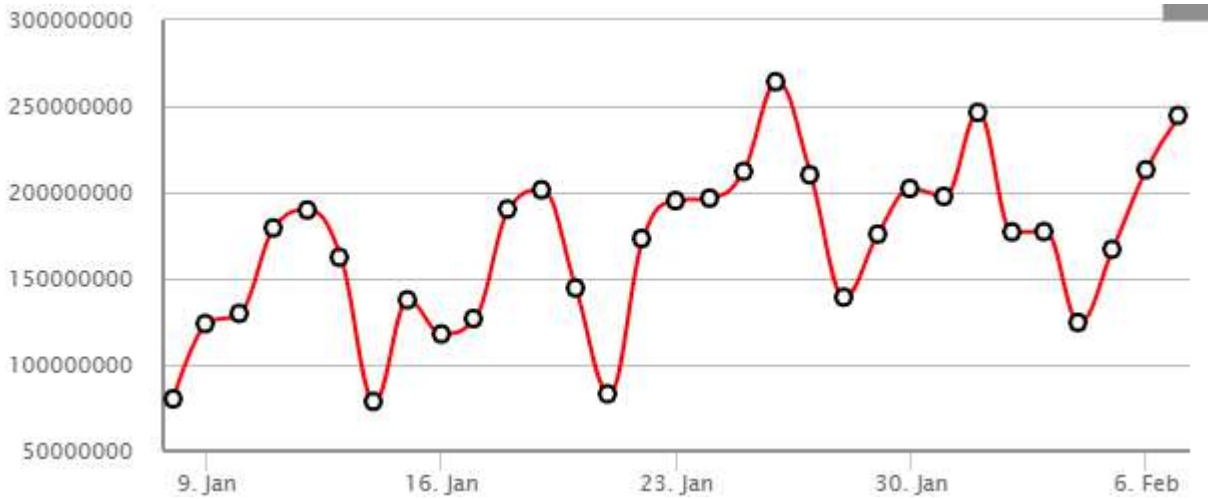

Рисунок 3 — Показатель спам атак в Российской Федерации за месяц

Сетевые атаки — это как правило, удаленное воздействие на компьютер с использованием программных методов. Целью подобных атак является нарушение конфиденциальности данных: кража информации, доступ к чужому компьютеру, изменение файлов. Такие атаки весьма сложны и потому их наименьшее количество, но ущерб от них колоссален. На графике ниже приведена активность сетевых атак за месяц в РФ (рисунок 4).

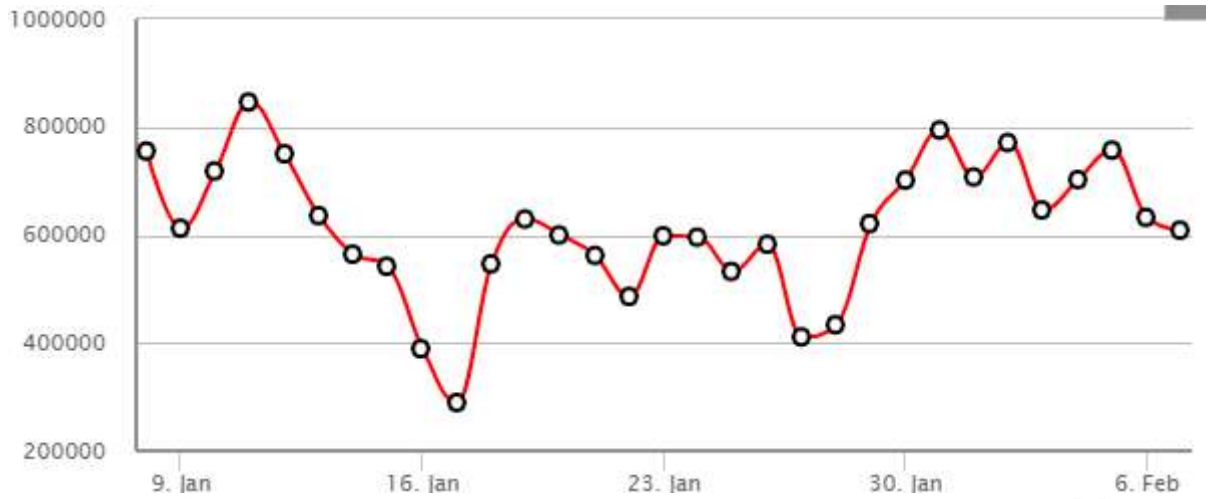

Рисунок 4. — Показатель сетевых атак в Российской Федерации за месяц [5]

Таким образом исходя из данных с графиков, можно сделать общую сводку информации и выразить в процентах (таблица 1).

Таблица 1. — Общая сводка угроз в Российской Федерации в процентах за месяц

Российская Федерация	
Угроза	Процент
Локальная	28.7%
Веб	17.5%
Спам	3.4%
Сетевая	2.4%

Помимо внешних угроз, нарушить безопасность могут и сотрудники организации.

Реализация вредоносных алгоритмов может привести к остановке системы, её сбоям, утере данных и подмене или утечке информации.

Таким образом, главными задачами систем информационной безопасности являются:

– возможность оперативного получения информационных услуг и обеспечение доступности данных для авторизованных пользователей;

– гарантия целостности информации — её актуальности и защищенности от несанкционированного изменения или уничтожения;

– обеспечение конфиденциальности данных.

Для решения представленных выше целей применяются такие методы защиты информации как: создание межсетевых экранов, криптография, аутентификация, регистрация, протоколирование и управление доступом.

Стоит отметить, что информационная безопасность также обеспечивается и государством, что отражается в требованиях нормативно-правовых актов, таких как:

1. Гражданский кодекс РФ.
2. Федеральный закон от 06.04.2011 г. № 63-ФЗ «Об электронной подписке».
3. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных».
4. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
5. Федеральный закон от 29.06.2004 г. № 98-ФЗ «О коммерческой тайне» [1].

Регуляторами в области информационной безопасности в РФ являются: Федеральная служба по техническому и экспортному контролю, Федеральная служба безопасности, Федеральная служба охраны, Министерство обороны РФ, Министерство связи и массовых коммуникаций РФ, Служба внешней разведки РФ и Банк России.

Так, регуляторами выдвигаются следующие требования к защите данных в компьютерных сетях:

– использование лицензионных технических средств и ПО;

– проведение проверки объектов информации на соответствие нормативным требованиям по защищенности;

– составление списка допустимых к применению программных средств и запрет на использование средств, не входящих в этот перечень;

– использование и своевременное обновление антивирусных программ, проведение регулярных проверок компьютеров на предмет заражения вредоносными ПО;

– разработка способов профилактики по недопущению попадания вирусов в сеть;

– разработка методов хранения и восстановления, зараженного ПО [2, 6].

Естественно, что государство не может обеспечить полную защиту информационной среди организации. Поэтому, каждой организации следует самим заботится о безопасности информации.

Рассмотрим методы и средства, которые необходимо применить для обеспечения безопасности информации организации.

Для обеспечения безопасности информации необходимо принять следующие меры:

– сформировать политику безопасности и составление соответствующей документации;

– внедрение технических средств защиты информации.

Для обеспечения целостной защиты информации в организации следует использовать технологии антивирусной защиты информации. Такое ПО направленно на экранирование рабочих сетей от несанкционированного враждебного ПО. Обеспечивает защиту рабочих станций, закрывает почтовые шлюзы, прокси-серверы и другие пути проникновения вирусов. В отличии от домашнего использование, в корпоративных условиях наиболее эффективным решением будет использование нескольких антивирусов, для обеспечения наибольшего диапазона блокируемых угроз [3].

Ещё одним эффективным методом обеспечения защиты информации в менеджменте являются межсетевые экраны. Такие экраны обеспечивают разделение сетей и устраняют нарушения пользователями установленных правил безопасности. Межсетевые экраны так же способны взаимодействовать с антивирусом и обеспечить возможности VPN для организации [4, 7].

Для любой серьезной организации необходимо внедрение системы обнаружения атак. Такие системы интегрированы со средствами блокировки вредоносных воздействий. Система акцентирует внимание администратора, только на тех угрозах, которые несут существенный ущерб организации. Минусом данной системы является весьма низкий скоростной показатель работы.

Повышения безопасности информации в организации можно также достигнуть путем контроля доступа и средств защиты информации внутри сети. В крупных компаниях с целью повышения безопасности создается автоматизация системы управления информационной безопасностью, через общую консоль. Обеспечивается разграничение доступа между сотрудниками согласно их функционалу. Одним из эффективных методов является создание корпоративного VPN, который обеспечивает более надежное шифрование трафика внутри организации.

Помимо вышеописанного, следует обратить внимание на стремительно развивающиеся системы обеспечения безопасности информации, которые используются для сохранения медиа контента от пиратства. На данный момент в сфере игровой индустрии существует система под названием «DENUVO».

«DENUVO» — это технология защиты от несанкционированного взлома, разработанная австрийской компанией «Denuvo Software Solutions GmbH».

«DENUVO», работает за счет того, что сама себя шифрует и расшифровывает. Делает это с достаточной периодичностью, чтобы взлом в большинстве случаев не представлялся возможным. Эта технология включает в себя «64-битную шифровальную машину», которая требует криптографические ключи, уникальные для конкретного оборудования каждой установленной системы.

Оборудование, защищенное «DENUVO» требует повторную онлайн-активацию для каждого обновления аппаратной части, делая 4 обновления за 24 часа. Данная система была взлома лишь один раз и на её взлом, причем конкретной программы, защищенной ей, ушел месяц у целой организации. Так что подобная система могла бы стать отличным вариантом для обеспечения безопасности информации в организации, а не только для сохранения медиа контента от пиратства.

Необходимо сказать пару слов о стоимости подобных методов защиты.

Цена организации корпоративной системы защиты сведений складывается из множества составляющих. В частности, она зависит от сферы деятельности компании, количества сотрудников и пользователей, территориальной распределенности системы, требуемого уровня защищенности и др. На стоимость работ влияет цена приобретаемого

оборудования и ПО, объем выполняемых работ, наличие дополнительных сервисов и другие факторы.

Так, стоимость программно-аппаратного комплекса Cisco WebSecurity варьируется от $170 (при количестве пользователей до 1000) до $670 (5000–10 000 пользователей). Локально развертываемое устройство McAfee WebGateway стоит от $2000 до $27000. Цена веб-фильтра Websense WebSecurity может достигать $40 000.

Стоимость Barracuda WebFilter стартует от $1500 за оборудование, обслуживающее до 100 пользователей одновременно (аппарат для обслуживания 300–8000 пользователей обойдется в $4000). При этом ежегодное обновление ПО обойдется еще в $400–1100. Приобрести GFI WebMonitor для 100 пользователей на один год можно за 208 000 рублей ($2600).

В данной статье были описаны основные нюансы информационной безопасности в корпоративных сетях, которые подвергаются наибольшему количеству угроз со стороны вирусных атак и человеческого фактора. Цель статьи была достигнута и предложен ряд методов, таких как: межсетевые экраны, антивирусное ПО, системы обнаружения атак и т.д. Всё это составляет комплексную защиту, которая способствует снижению риска несанкционированного доступа к рабочей информации и оптимизации общего рабочего процесса. Помимо этого, в статье была рассмотрена технология «DENUVO», которая в перспективе способна стать частью стандартного комплекса защиты повысив его эффективность.

Литература

1. Гражданский кодекс Российской Федерации: Часть первая – четвертая: [Принят Гос. Думой 23 апреля 1994 года, с изменениями и дополнениями по состоянию на 10 апреля 2009 г.] // Собрание законодательства РФ. — 1994. — № 22. — Ст. 2457.

2. Лопатин, В. Н. Информационная безопасность России: Человек, общество, государство. Серия: Безопасность человека и общества / В. Н. Лопатин. — М.: 2008. — 428 с.

3. Родионов, М. А. Методологические аспекты информационного аудита в менеджменте предприятия / М. А. Родионов. — Научный Вестник МГТУ ГА. — 2009. — № 156. — С. 68–74.

4. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. — М. : ДМК Пресс, 2008. — 544 с.

5. АО «Лаборатория Касперского»: официальный сайт [Электронный ресурс] — Режим доступа: https://securelist.ru/statistics/

6. Мухин, Д. Э., Столяренко А. В. Информационно-коммуникационная среда туристско-рекреационного предприятия Крыма // Таврический научный обозреватель. — 2017. — №1 (18) [Электронный ресурс]. — Режим доступа: http://tavr.science/stat/2017/01/08-Stolyarenko_Muhin.pdf

7. Столяренко, А. В. Применение информационно-коммуникационных технологий в деятельности предприятий туристской сферы / А. В. Столяренко, А. А. Данильченко // Современные научные исследования и инновации, 2017. — №1. — [Электронный ресурс]. — Режим доступа: http://web.snauka.ru/issues/2017/01/77660