

## УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Жебричук А.В., Ниценко В.С.

**Аннотация.** В статье приведен анализ современных угроз информационной безопасности компании. Рассмотрены угрозы информационной безопасности. Предоставлены пути защиты информации в компании.

**Abstract.** The article provides an analysis of contemporary threats to information security. Considered threats to information security. Given the way the protection of information in the company.

**Ключевые слова:** информационная безопасность, угрозы, инсайдеры, кибератака.

Деятельность любой организации в наше время связана с получением и передачей информации. Информация является сейчас стратегически важным товаром. Доступ к информационным ресурсам или завладение секретной информацией конкурентами, как правило, наносит предприятию значительный ущерб и даже может привести к банкротству. За последние 20 лет информационные технологии (ИТ) проникли во все сферы управления и ведения бизнеса. Сам же бизнес из реального мира, давно переходит в мир виртуальный, а поэтому весьма зависим от вирусных, хакерских и прочих атак. По данным Института Компьютерной Безопасности общий ущерб, который нанесли компьютерные вирусы за последние 5 лет, оценивается как минимум в 70 млрд. долл. Также появилась ещё одна проблема информационной безопасности (ИБ) – спам. Это анонимная массовая непрошенная рассылка. Сейчас около 30% всех электронных писем являются спамом. Наводнение спама приводит к ежегодным убыткам, оцененным до 20 млрд. долл. Спам в пределах одной компании, приводит к убыткам от 600 до 1000 долл. ежегодно, из расчета на одного пользователя. Широко распространяется сейчас промышленный шпионаж – устройство стоимостью всего 10 долл., в случае его удачного размещения, может привести фирму к банкротству.

Анализ актуальных угроз конфиденциальной информации начинается с понимания и классификации этих угроз. Под угрозой информационной безопасности понимается потенциальная возможность нарушения основных качеств или свойств информации – доступности, целостности и конфиденциальности. Угрозы информационной безопасности делят на две категории – внешние и внутренние угрозы. Данная классификация предусматривает разделение угроз по локализации злоумышленника (или преступной группы), который может действовать как удалённо, пытаясь получить доступ к конфиденциальной информации предприятия при помощи сети интернет, либо же действовать посредством доступа к внутренним ресурсам ИТ-инфраструктуры объекта. В случае внешних атак, преступник ищет уязвимости в информационной структуре, которые могут дать ему доступ к хранилищам данных, ключевым узлам внутренней сети, локальным компьютерам сотрудников. В этом случае злоумышленник пользуется широким арсеналом инструментов и вредоносного программного обеспечения (вирусы, трояны, компьютерные черви) для отключения систем защиты, шпионажа, копирования, фальсификации или уничтожения данных, нанесения вреда физическим объектам собственности и т.д. Внутренние угрозы подразумевают наличие одного или нескольких сотрудников предприятия, которые по злему умыслу или по неосторожности могут стать причиной

утечки конфиденциальных данных или ценной информации. Рассмотрим эти категории рисков информационной безопасности подробнее.

Доклад Всемирного экономического форума «Глобальные риски» («Global Risks») рассматривает кибератаки как одну из основных угроз. По вероятности наступления, кибератаки входят в пятерку наиболее вероятных глобальных угроз. Такое заключение Всемирного экономического форума свидетельствует о высокой актуальности и значительной опасности электронной преступности. Итак, кибератаки сегодня – давно не голливудский миф, это реальная и серьезная опасность информационной инфраструктуре, интеллектуальной и физической собственности государственных и коммерческих объектов. Наиболее распространённой и разнообразной по методам исполнения формой киберпреступности является использование вредоносного программного обеспечения (ПО). Такие угрозы представляют прямую опасность конфиденциальности и целостности информационных ресурсов организации. В атаках с использованием вредоносных кодов и приложений используются уязвимости информационных систем для осуществления несанкционированного доступа к базам данных, файловой системе локальной корпоративной сети, информации на рабочих компьютерах сотрудников. Спектр угроз информационной безопасности, вызванных использованием вредоносного программного обеспечения чрезвычайно широк. Вот некоторые примеры таких угроз защиты информации:

- внедрение вирусов и других разрушающих программных воздействий;
- анализ и модификация/уничтожение установленного программного обеспечения;
- внедрение программ-шпионов для анализа сетевого трафика и получения данных о системе и состоянии сетевых соединений;
- использование уязвимостей ПО для взлома программной защиты с целью получения несанкционированных прав чтения, копирования, модификации или уничтожения информационных ресурсов, а также нарушения их доступности;
- раскрытие, перехват и хищение секретных кодов и паролей;
- чтение остаточной информации в памяти компьютеров и на внешних носителях;
- блокирование работы пользователей системы программными средствами т.д.

Большинство инцидентов ИБ связано с воздействием внутренних угроз – утечки и кражи информации, утечки коммерческой тайны и персональных данных клиентов организации, ущерб информационной системе связаны, как правило, с действиями сотрудников этой организации. В классификации внутренних угроз в первую очередь можно выделить две большие группы – совершаемые из корыстных или других злонамеренных соображений, и совершаемые без злого умысла, по неосторожности или технической некомпетентности. Итак, преступления сотрудников, способных причинить вред сохранности интеллектуальной и коммерческой собственности организации (их принято называть «инсайдерами») можно разделить на категории злонамеренного инсайда и непредумышленного инсайда. Злоумышленным инсайдером могут стать:

- Сотрудники, затаившие злобу на компанию-работодателя («обиженные»). Такие инсайдеры действуют исходя из мотивов личной мести, причин для которой может быть масса – от увольнения/понижения в должности до отказа компании предоставить статусные атрибуты, например, ноутбук или расширенный соцпакет.

- Нечистые на руку сотрудники, стремящиеся подзаработать за счёт компании-работодателя. Такими инсайдерами становятся сотрудники, использующие секретные информационные ресурсы компании для собственной выгоды. Базы данных клиентов, интеллектуальная собственность компании, состав коммерческой тайны – такая информация может использоваться инсайдером в личных интересах, либо продаваться конкурентам.

- Внедрённые и завербованные инсайдеры. Самый опасный и самый трудно-идентифицируемый тип внутренних злоумышленников. Как правило, являются звеном преступной цепочки или членом организованной преступной группы. Такие сотрудники имеют достаточно высокий уровень доступа к конфиденциальной информации, ущерб от их действий может стать фатальным для компании.

Злонамеренные инсайдеры представляют определённую опасность для информационной системы и конфиденциальных данных, однако вероятность злоумышленных инцидентов ничтожно мала по сравнению с утечками информации, совершаемыми по неосторожности или вследствие технической безграмотности сотрудников. Да, увы, это так – львиная доля всех инцидентов информационной безопасности на объекте любой сложности является следствием непредумышленных действий сотрудников. Традиционные средства защиты (антивирусы, фаерволы и т.д.) на сегодняшний день не способны эффективно противостоять современным киберпреступникам.

Для защиты информационной системы организации требуется комплексный подход, сочетающий несколько рубежей защиты с применением разных технологий безопасности. Для защиты от внешних интернет угроз информационной безопасности отлично зарекомендовали себя системы предотвращения вторжений на уровне хоста (HIPS). Правильно настроенная система даёт беспрецедентный уровень защищённости, близкий к 100%. Грамотно выработанная политика безопасности, применение совместно с HIPS других программных средств защиты информации (например, антивирусного пакета) предоставляют очень высокий уровень безопасности. Организация получает защиту практически от всех типов вредоносного ПО, значительно затрудняет работу хакера, решившего попробовать пробить информационную защиту предприятия, сохраняет интеллектуальную собственность и важные данные организации.

Защита от внутренних угроз также требует комплексного подхода. Он выражается в выработке должных политик информационной безопасности, введением чёткой организационной структуры ответственных за информационную безопасность сотрудников, контроле документооборота, контроле и мониторинге пользователей, введении продвинутых механизмов аутентификации для доступа к информации разной степени важности. Степень такой защиты зависит от объективных потребностей организации в защите информации. Оптимальным выбором для большинства компаний станет введение функционала защиты от утечек данных, контроле документооборота и мониторинг действий пользователей локальной сети организации. Такое решение является недорогим, простым в развёртывании и эксплуатации, но весьма эффективным инструментом информационной безопасности.

#### **Литература:**

1. Галатенко В.А. Основы информационной безопасности. - М.: "Интуит", 2013.
2. Коуров Л.В. Основы обеспечения безопасности информационных систем. - М.: ИУП, 2010. – 60 с.

3. Щербаков А.О. Введение в теорию и практику компьютерной безопасности. - М.: "Издатель Молгачева С.В.", 2001. - 352 с.

## ОПЫТ ПРОИЗВОДСТВЕННОГО КООПЕРИРОВАНИЯ В ДЕРЕВНЕ УДМУРТИИ В 1920-Е ГГ.

Замятина Н.А., Емелина Т.Г.

**Аннотация.** В статье раскрываются факты и практика производственного кооперирования крестьянства в Удмуртской деревне в период новой экономической политики.

**Abstract.** The article reveals the facts and the practice of clustering of the peasantry in the Udmurt village in the period of the New Economic Policy.

**Ключевые слова:** история, производственная и потребительская кооперация, крестьянство, удмуртская деревня.

История потребительской кооперации крестьянства Удмуртии представляет значительный интерес для специалистов, но не менее содержательной были страницы истории производственной кооперации. Поскольку характерной особенностью деревни Удмуртии начала XX века являлась устойчивость общинных социально-экономических институтов, это, по мнению властей того времени, облегчало реализацию аграрную политику большевиков в деревне Удмуртии. Через систему политических, экономических и культурных мероприятий оно пыталось сформировать у крестьян убеждения о выгодах производственной сельскохозяйственной кооперации. Главным аргументом стали успехи потребительской кооперации. Перед властью стояла задача осуществить переход от потребительского кооперирования к производственному кооперированию. Опыт производственного кооперирования формировался с помощью организации проката машин и средств производства, организованной в рамках потребительской кооперации. Использование инвентаря прокатных пунктов приводило к созданию многообразных простейших форм совместного труда

Анализ опыта появления и функционирования первых производственных коллективных хозяйств позволяет выделить несколько этапов в истории этого вопроса в области. Первые производственные кооперативы появились в области на фоне революционных событий и представляли собой коммуны. Данные коммуны быстро прекратили свое существование в условиях Гражданской войны. Колхозное движение ВАО, начавшееся в 1918 и продолжавшееся вплоть до 1924 года, развивалось стихийно, было предоставлено само себе, не испытывало руководства со стороны областных и уездных комитетов партии и поэтому не получило заметного развития.

Следующий этап производственной кооперации связан с осуществлением новой экономической политики в нашем крае. Данный исторический опыт заслуживает более детального изучения. Выход сельского хозяйства области из кризиса, последовавшего за Гражданской войной, и мероприятия государственной кредитной поддержки производственной кооперации способствовали появлению коллективных хозяйств в области. Доля возникших производственных объединений в сельском хозяйстве Удмуртии была