Селехова Анастасия Алексеевна

студентка специальности «Экономическая безопасность» Тюменского государственного университета, г. Тюмень, n.selehova@yandex.ru

Лаубах Карина Сергеевна

студентка специальности «Экономическая безопасность» Тюменского государственного университета, г. Тюмень, karina.laubah@yandex.ru

РЕЖИМ КОММЕРЧЕСКОЙ ТАЙНЫ И КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ ХОЗЯЙСТВУЮЩЕГО СУБЪЕКТА

Аннотация. Статья посвящена установлению слабых сторон разных компании, которые могут привести к рискам потери коммерческой тайны, что впоследствии, негативно повлияет на результаты и приведёт к убыткам. В статье рассматривается понятие компьютерной безопасности, как части экономической безопасности. Представляется определение коммерческой тайны и раскрывается режим коммерческой тайны хозяйствующего субъекта.

Ключевые слова: коммерческая тайна, информационная безопасность, компьютерная безопасность, экономическая безопасность, конфиденциальность.

Selekhova Anastasia Alekseevna

Student of the specialty "Economic Security", Tyumen State University, Tyumen, n.selehova@yandex.ru

Laubah Karina Sergeevna

Student of the specialty "Economic Security", Tyumen State University, Tyumen, karina.laubah@yandex.ru

TRADE SECRET REGIME AND COMPUTER SECURITY OF A COMPANY

Abstract. The article is devoted to identifying the weaknesses of different companies that may lead to the risk of losing trade secrets, which subsequently, negatively affect the results and lead to losses. The article considers the concept of computer security as part of economic security. The definition of trade secrets is presented and the regime of trade secrets of the business entity is disclosed.

Keywords: trade secrets, information security, computer security, economic security, confidentiality.

Предпринимательство является одной из самых важных сфер деятельности современной экономической системы. Она не стоит на месте и постоянно развивается, включая в себя все новые направления, но некоторые из них остаются неизменными.

Коммерческая тайна является неотъемлемым свойством как рыночной экономики, так и деятельности организации. Очевидно, что за время действия предпринимательской деятельности накапливается большое количество разнообразной информации, которая связана с успешным развитием бизнеса и если данная информация обнародуется, то, скорее всего, предприятие будет далеко не в выигрышном состоянии, поэтому необходимо соблюдать коммерческую тайну и контролировать её, так как в современном мире, информация приобретает значение важного и является одним из главных ресурсов, без которого сложно представить разумное функционирование ни отдельного предпринимателя, ни общества и государства в целом.

Современный этап развития бизнеса подразумевает подкрепления своей безопасности при помощи улучшения и своевременного обновления системы защиты персональных данных и облачного хранения.

Мы считаем, что компьютерная безопасность – это важный аспект современной жизни людей, при переходе многих сфер предоставления товаров и услуг на удаленную работу, многие владельцы крупных бизнесов задумались о дополнительной безопасности своего дела. Одним из ключевых интересов владельца бизнеса является сохранение и, по возможности, увеличение ценности, управляемой им компании. В настоящее время компьютерная безопасность на предприятии стала подвергаться большим количеством атак со стороны мошенников, что ставит под угрозу сохранность ее коммерческой тайны.

Конфиденциальность информации организации зависит от коммерческой тайны, ведь именно она позволяет обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке или получить иную коммерческую выгоду.

Коммерческая тайна – это умышленно скрываемые экономические интересы и данные о различных сферах производственно-хозяйственной, управленческой и финансовой деятельности организации.

В связи с тем, что развитие предпринимательской деятельности происходит в условиях быстрой изменчивости экономической среды, а также быстрого развития информационных технологий, то возникает неуверенность в получении ожидаемого конечного результата, а значит, увеличится риск непредвиденных потерь. В целях обеспечения эффективного функционирования предприятия перед предпринимателем

встает задача разработать отлаженную систему обеспечения экономической безопасности хозяйствующего субъекта [1].

Сегодня обеспечение экономической безопасности показывает уровень успешного функционирования и развития всех элементов хозяйствующего субъекта. Одним из таких элементов в современное время все большую значимость приобретает компьютерная безопасность или другими словами информационная безопасность.

В настоящее время понятие компьютерные преступления в научной литературе, по мнению Зверевой Е.Б., звучит так: «Компьютерные преступления - любое противоправное действие, при котором компьютер выступает либо как объект, против которого совершается преступление, либо как инструмент, используемый для совершения преступных действий». Само значение за долгое время не изменилось и все так же это остается опасной частью бизнеса, которую стоит улучшать и подкреплять [2].

Целью компьютерной безопасности является обеспечение надежной защиты компьютеров, серверов, сетей, мобильных устройств и информации, хранящихся на этих устройствах, от злоумышленников. Кибератаки могут быть предназначены для доступа, удаления или вымогательства конфиденциальных сведений организации или пользователя, делая кибербезопасность очень важной.

В зависимости от различных способов классификации, на наш взгляд, все возможные угрозы компьютерной безопасности можно разделить на следующие основные подгруппы: нежелательный контент, несанкционированный доступ, утечки информации, потеря данных, мошенничество. Для наглядности масштабов компьютерных преступлений представлены данные на основе атак произведенных на предприятия за 2019 год (рисунок 1).

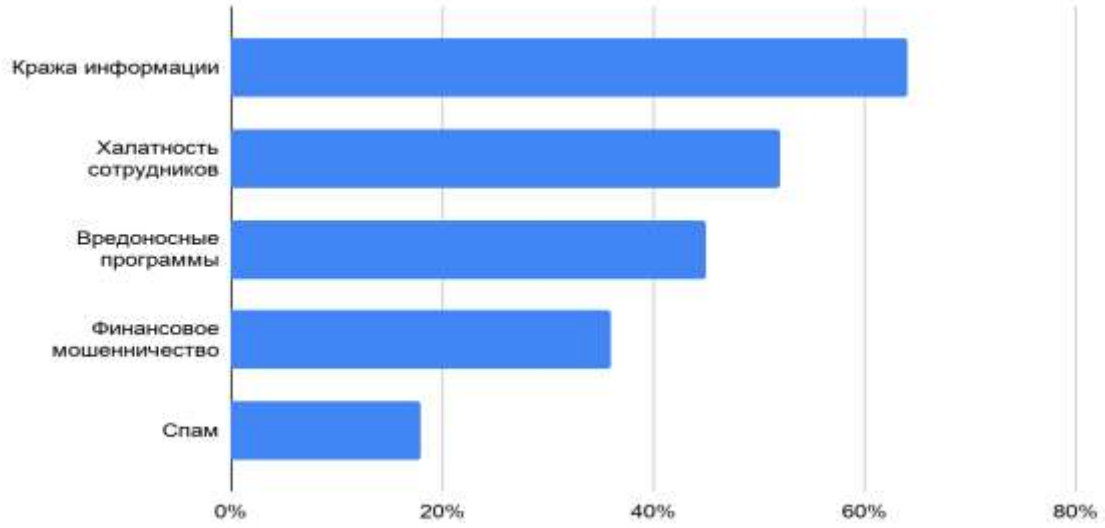

Рисунок 1. Угрозы компьютерной безопасности

Источник: составлено авторами на основе [3]

Утечки информации можно разделять на умышленные и случайные. Случайные утечки происходят из-за ошибок оборудования, программного обеспечения и персонала. Умышленные, в свою очередь, организовываются преднамеренно с целью получить доступ к данным, нанести ущерб.

Потерю данных можно считать одной из основных угроз информационной безопасности. Нарушение целостности информации может быть вызвано неисправностью оборудования или умышленными действиями людей, будь то сотрудники или злоумышленники.

Потерю данных можно считать одной из основных угроз информационной безопасности. Нарушение целостности информации может быть вызвано неисправностью оборудования или умышленными действиями людей, будь то сотрудники или злоумышленники.

Не менее опасной угрозой является мошенничество. К мошенничеству можно отнести не только манипуляции с кредитными картами, но и взлом онлайн-банка. Целями этих экономических преступлений являются обход законодательства, политики безопасности или нормативных актов, присвоение имущества.

На сегодняшний день никого не удивляет возможность атак на автоматизированные системы управления технологическими процессами различных предприятий. Любая информация того или иного хозяйствующего субъекта в процессе предпринимательской деятельности может представлять интерес для третьих лиц таких как: конкуренты, правонарушители, шпионы и т.д. Именно поэтому важно применять меры соблюдения и контроля над стабильной защитой компьютерной безопасности, иначе это может привести к нарушению коммерческой тайны, а следствие к промышленному шпионаж [4].

На наш взгляд, никакие самые надежные меры не смогут обеспечить стопроцентную защиту от компьютерных вирусов и программ, но, выработав для себя ряд правил, вы существенно снизите вероятность вирусной атаки и степень возможного ущерба.

Одним из основных методов борьбы с вирусами является, своевременная профилактика. Компьютерная профилактика состоит из небольшого количества правил, соблюдение которых значительно снижает вероятность заражения вирусом и потери каких-либо данных.

Одним из самых эффективных способов повысить общий уровень информационной безопасности – это развивать и поддерживать высокий уровень информационной культуры и общей культуры делопроизводства. Очевидно, что чаще крадут информацию там, где присутствует необязательность и бесконтрольность. В этом случае труднее понять, что на

самом деле произошло, труднее собрать фактический материал для внутреннего расследования, а злоумышленнику легче скрыть следы.

В России рынок высокотехнологичных преступлений в финансовой сфере сократился на 85%. Исследователи отмечают, что сокращение в России ущерба от всех видов киберпреступлений, направленных как напрямую на банки, так и их клиентов привело к рекордному падению рынка на 85% [5].

Согласно оценке аналитиков, рынок высокотехнологичных преступлений в финансовой отрасли России, сократился до 510 млн рублей за период 2018 — 2019 против 3,2 млрд рублей в предыдущем периоде, а также стоит отметить, что в России растет количество преступлений против клиентов банков с использованием социальной инженерии и телефонного, компьютерного мошенничества [5].

Для наглядности масштабов компьютерных преступлений данные представлены в таблице 1. Согласно отчету, до 93 млн руб, то есть почти в 14 раз сократились потери от целевых атак на банки в России со стороны финансово мотивированных группировок. По сравнению с прошлым периодом, средняя сумма хищения от целевых атак на банки в России упала со 118 до 31 миллиона рублей [5].

Таблица 1

Рынок высокотехнологичных преступлений в финансовой отрасли России за 2018-2019 гг.

Сегмент рынка в России	Количество групп	Общее число успешных атак	Средняя сумма одного хищения (в руб.)	Средняя сумма хищения (в руб.)	2018-2019 гг. (в руб.)
Хищение у юридических лиц, с троянами для ПК	2	0,5	500 000	250 000	62 250 000
Хищение у физических лиц с Android троянами	5	40	11 000	440 000	109 560 000
Целевые атаки на банки	3	-	31 000 000	-	93 000 000
Обналичивание похищенных средств	-	-	-	467 100	158 157 900
Итого	-	-	-	1 157 100	422 967 900

Источник: составлено авторами на основе [5]

Полноценное обеспечение информационной безопасности на предприятии должно быть стандартизировано и находиться под полным контролем круглосуточно. Полномочия службы информационной безопасности распространяются на установление порядка рассекречивания и уничтожения информации, которая находилась под защитой.

Отдел компьютерной безопасности контролирует различные сведения, относящиеся к коммерческой тайне компании. Такими сведениями могут выступать: публикуемая информация, обеспечивающая технические средства защиты, договоры с контрагентами, картотеки клиентов и поставщиков, операции с ценными бумагами, данные финансово-бухгалтерской отчетности, схемы финансовых операций и т.д. К сведениям составляющим коммерческую тайну также может быть отнесена информация управленческого характера, таких как: структура и методы управления компанией, схемы управления производством, сведения о заработной плате, информация о наличии свободных мест, решения кадровых вопросов и т.д.

Авторы считают, чтобы корректно защищать конфиденциальные данные предприятия, необходимо определить перечень информации, входящий в коммерческую тайну того или иного предприятия. Разглашение коммерческой тайны может повлечь за собой привлечение сотрудников к гражданской, административной или уголовной ответственности. Если сотрудник разгласил коммерческую тайну, нарушив условия трудового договора, то он обязан возместить все убытки, причем не только те, что вызвали реальный ущерб, но и упущенную выгоду. Похожий путь будет не только для сотрудников, но также для граждан и предприятия, которые узнали информацию незаконно.

Для защиты интересов обладателя информации, представляющей коммерческую тайну предусмотрены ряд законов позволяющие обеспечить наказания нарушителям. В ряд таких законов входят: Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ; Федеральный закон № 149-ФЗ от 27 июля 2006 года «Об информации, информационных технологиях и о защите информации»; Федеральный закон № 152-ФЗ от 27 июля 2006 года «О персональных данных».

Все установленные меры в данных федеральных законах могут применяться в отношении как государственных, так и муниципальных организаций, а также контрагентов и нарушителей со стороны. Для предпринимателя наибольшее значение имеет гражданско-правовая ответственность так, как благодаря ей можно в полной мере возместить убытки, причиненные после распространения конфиденциальной информации, составляющую коммерческую тайну [6].

Стоит отметить, что правильно организованный и хорошо защищенный режим коммерческой тайны на предприятии, подкрепленный законодательством, напрямую может

обеспечить информационную безопасность данного предприятия, ведь именно при достаточной конфиденциальности сведений можно обеспечить их сохранность.

Библиографический список

1. Головкина Д.В. Обеспечение информационной безопасности установлением режима коммерческой тайны // Вестник Прикамского социального института. 2019. № 1(82). С. 12-16.

2. Зверева Е.Б. Киберпреступность как угроза безопасности современного общества: виды, особенности, методы борьбы и профилактики // Молодой ученый: [сайт]. [дата публ. 05.02.2019]. URL: https://moluch.ru/archive/300/67972/ (дата обращения: 13.03.2021).

3. Угрозы компьютерной безопасности // Anti-malware: [сайт]. [дата публ. 09.12.2019]. URL: https://www.anti-malware.ru/threats/information-security-threats (дата обращения: 01.04.2021).

4. Информационная безопасность бизнеса // Справочник автора: [сайт]. [дата публ. 06.10.2019]. URL: https://spravochnick.ru/ekonomika/suschnost_ekonomicheskoy_bezopasnosti/ekonomicheskaya_bezopasnost_hozyaystvuyuschego_subekta/ (дата обращения: 25.03.2021).

5. Group-IB: количество атак прогосударственных и финансово мотивированных хак-групп растёт // Информационный портал xakep.ru: [сайт]. [дата публ. 02.12.2019]. URL: https://xakep.ru/2019/12/02/hi-tech-crime-trends-2019-2020/ (дата обращения: 01.04.2021).

6. Пронин К.В. Защита коммерческой тайны. Москва: ГроссМедиа, 2006. 228 с.