РОЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЗАЩИТЕ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ И ВЛИЯНИЕ НА ЭКОНОМИЧЕСКУЮ БЕЗОПАСНОСТЬ РЕГИОНА

Лимановская В.Р.
Федеральное государственное бюджетное научное учреждение «Институт научно-технической информации», г. Донецк

Аннотация. В статье изучается важность информационной безопасности в контексте защиты интеллектуальной собственности и ее воздействие на экономическую безопасность региона. В условиях цифровой трансформации бизнеса информационная безопасность становится ключевым элементом защиты ценных активов компании, включая интеллектуальные ресурсы.

Ключевые слова: информационная безопасность, интеллектуальная собственность, экономическая безопасность региона, защита данных.

В условиях цифровой трансформации бизнеса информационная безопасность становится неотъемлемым элементом защиты ценных активов организации, включая интеллектуальную собственность. В данной статье исследуется значение информационной безопасности как фундаментального элемента защиты интеллектуальной собственности, а также влияние информационной безопасности предприятий на экономическую безопасность региона.

В данной статье под интеллектуальной собственностью предприятия понимаются не только зарегистрированные объекты интеллектуальной собственности, но и служебные результаты интеллектуальной деятельности, а также информация о предприятии, которая не подлежит разглашению.

Определим взаимосвязь интеллектуальной собственности и

информационной безопасности, а также их влияние на экономическую безопасность в регионе. Направления взаимосвязи информационной безопасности и интеллектуальной собственности на разных уровнях представлены в таблице 1.

Таблица 1 – Направления взаимосвязи интеллектуальной собственности и информационной безопасности

Уровень предприятия Направление	Характеристика
Защита конфиденциальности данных	Обеспечение безопасности хранения и обработки конфиденциальной информации важно для предотвращения утечек и сохранения интеллектуальной собственности организации.
Управление доступом	Регулирование доступа к ценной информации с целью предотвращения несанкционированных действий персонала или внешних агентов, что может привести к утрате интеллектуальной собственности.
Мониторинг активности	Постоянный мониторинг действий сотрудников и внешних угроз позволяет своевременно обнаруживать и предотвращать инциденты, которые могут негативно отразиться на интеллектуальной собственности.
Обмен опытом и информацией	Создание механизмов для обмена информацией о киберугрозах и методах защиты интеллектуальной собственности между компаниями в регионе способствует повышению уровня информационной безопасности.
Создание образовательных программ	Развитие учебных программ и инициатив по обучению населения в области информационной безопасности способствует повышению осведомленности о киберугрозах и защите интеллектуальной собственности.
Проведение семинаров и тренингов	Организация мероприятий по обмену опытом и повышению компетенций в сфере информационной безопасности помогает создать сильную защитную систему для интеллектуальной собственности на уровне региона.

Создание взаимодействия между информационной безопасностью и защитой интеллектуальной собственности как в организации, так и в регионе, позволит эффективно обезопасить ценные активы от угроз, поможет предотвращать кражу инноваций и сохранить конкурентные преимущества, что способствует экономической безопасности региона.

Основными угрозами для информационной безопасности являются: утечка данных, в том числе и об интеллектуальной собственности компаний; повреждение репутации в следствие утечки данных; киберугрозы, кибератаки и др.

Юнусова Д. А. и Дахададаева А. А. в своей работе [1] выделили такие негативные воздействия: «утрата доступа, потеря связи с провайдером услуг, изменение или модификация данных, замена и фальсификация информации, распространение вредоносного программного обеспечения, создание вымышленной информации, уничтожение или ограничение доступа к данным, отключение важных компонентов интернет-ресурсов, внедрение вредоносного кода, ограничение доступа к ресурсам и т.п.»

Утечка конфиденциальной информации может привести к серьезным финансовым потерям для организации, особенно если утрачены ключевые инновации или технологии. Инциденты утечки данных наносят ущерб репутации компании. Аналитики «Инфосистемы Джет», организации по аутсорсингу информационной безопасности, в отчете за 2023 год представили топ-10 случаев утечки данных (табл. 2) [2].

Таблица 2 – Топ-10 распространенных техник MITRE ATT&CK в 2023 г.

Название метрики	Краткая характеристика	Объем (%)
User Execution	Инциденты, связанные с заражением узлов вредоносными программами (в том числе массовыми), а также обнаружением индикаторов компрометации в защищаемом периметре.	34,63%
Impair Defenses, Disable or Modify Tools	Кодификация и отключение средств защиты (чаще всего — средств АВЗ). Случаи отключения антивирусных агентов. Переходом антивирусных агентов в «критический» статус, который в основном связан с устареванием антивирусных баз или невозможностью агента соединиться с сервером управления. Преднамеренное отключение как устанавливаемых средств защиты, так и встроенных.	27,60%
Exploit Public-Facing	Инциденты связаны с эксплуатацией публично	17,33%

Application	доступных веб-приложений.	
Brute Force, Password Guessing	Инциденты, связанные с методами брутфорса и угадывания паролей. Нетипичные аутентификации, внутренние и внешние попытки подбора паролей, нетипичные действия с учетными данными и нетипичный удаленный доступ.	8,21%
External Remote Services	К данному типу относятся инциденты, связанные с атаками на внешние сервисы, такие как VPN, VNC и другие. Зачастую после таких атак злоумышленники также могли получить доступ к внутренней инфраструктуре.	4,82%
Password Spraying	Инциденты данной категории связаны с использованием метода подбора паролей, когда один пароль тестируется для множества собранных ранее учетных записей.	1,37%
Application Layer Protocol, DNS	Категория вредоносной сетевой активности, которая включает в себя атаки с применением протоколов прикладного уровня и DNS. DNS — один из наиболее распространенных видов трафика, который генерируется в инфраструктуре.	1,14%
Proxy: Multi-hop Proxy	Инциденты, связанные с использованием прокси с множественными прыжками (например, сети Tor и i2p). Часто Tor и другие многоуровневые сети применяются злоумышленниками для сокрытия реального адреса атаки или как средство для обратной коммуникации (backdoor).	0,91%
Remote Services	Инциденты, связанные с удаленными службами, когда уже из защищаемого периметра осуществляется нелегитимное обращение к внешним сервисам удаленного администрирования.	0,76%
Remote Access Software	Инциденты, связанные с программным обеспечением удаленного доступа.	0,37%

Для защиты информации и интеллектуальной собственности в организации важно не только иметь качественное программное обеспечение, но и обученный, грамотный персонал. Необходимо реализовывать базовые мероприятия по обеспечению информационной безопасности (табл. 3).

Таблица 3 – Мероприятия по обеспечению информационной

безопасности

Мероприятия	Характеристика	Результат
Регулярное обновление систем защиты:	Внедрение современных технологий защиты данных и постоянное обновление систем позволяют удерживать уровень информационной безопасности на высоком уровне.	Защита от кибератак и хакерских атак: Мощные системы защиты могут предотвратить атаки на информацию и инфраструктуру, что является важным аспектом для сохранения интеллектуальной собственности. Предотвращение утечек конфиденциальной информации предприятий способствует сохранению экономической безопасности региона в целом, предотвращает экономические потери и сохраняет конкурентоспособность.
Обучение персонала:	Проведение обучающих программ и тренингов по правилам безопасности помогает повысить осведомленность сотрудников и уменьшить человеческий фактор в утечках данных.	Предотвращение утечки конфиденциальной информации: Эффективные меры информационной безопасности помогают предотвратить утечку и незаконное распространение ценных знаний и технологий компании.
Повышение уровня компьютерной грамотности сотрудников.	Процесс обучения и развития знаний, навыков и умений персонала по эффективному и безопасному использованию компьютеров, программного обеспечения и информационных технологий в рабочей деятельности.	Знание о методах киберзащиты, правилах работы с конфиденциальной информацией и этике в цифровом пространстве способствует предотвращению кражи интеллектуальной собственности и нарушению авторских прав. Повышение уровня защиты предприятий от киберугроз снижает вероятность масштабных кибератак на компании в регионе, что в конечном итоге способствует экономической стабильности.
Содействие в создании благоприятной инвестиционной среды	Комплекс мероприятий и политических действий, обеспечивающих условия, способствующих привлечению инвестиций, созданию благоприятной атмосферы для вложения капитала, развитию предпринимательства и стимулированию экономического роста.	Высокий уровень информационной безопасности предприятия создает доверие у потенциальных инвесторов и партнеров, обеспечивая благоприятные условия для инвестиций. Что в свою очередь способствует развитию экономики, и укрепляет экономическую безопасность региона.

Реализация подобных мероприятий поможет сохранить данные на уровни компании и в совокупности повлиять на улучшение

экономической стабильности в любом регионе.

Подводя итог, информационная безопасность играет решающую роль в обеспечении защиты интеллектуальной собственности организации. Успешная реализация мер по обеспечению безопасности данных способствует сохранению основных активов компании и обеспечению ее стабильности и конкурентоспособности в долгосрочной перспективе.

Связь между информационной безопасностью на уровне предприятия и экономической безопасностью на уровне региона напрямую влияет на устойчивое развитие бизнеса и экономики. Предприятия, обеспечивающие высокий уровень информационной безопасности, способствуют укреплению экономической безопасности региона в целом.

Список использованных источников

1. Юнусова Д. А. Информационная безопасность региона / Д. А. Юнусова, А. А. Дахададаева // Индустриальная экономика. – 2022. – №3. – URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-regiona

2. Итоги года 2023 // jetcsirt.su – URL: https://jetcsirt.su/upload/godovoy_otchet__jet_2023.pdf

Контактная информация:
Лимановская Вероника Романовна
E-mail: naali20@mail.ru