УДК 005.5

Першикова Е.Д., Суслова В.С., Волкова Д.Г.,
студенты факультета экономики и управления,
Московский государственный университет технологий и управления
им. К.Г.Разумовского

Научный руководитель: Швеёва Е.И., к.э.н.,
Московский государственный университет технологий и управления
им. К.Г.Разумовского
г.Москва, Россия

МЕНЕДЖМЕНТ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК НЕПРЕРЫВНЫЙ ПРОЦЕСС

Аннотация: *В данной статье рассматривается управление рисками информационной безопасности как непрерывный процесс, который требует интеграции в стратегическое планирование организаций. Анализируются ключевые этапы управления рисками: идентификация, оценка, реагирование и мониторинг. Особое внимание уделяется уязвимостям в цифровой среде и на промышленных предприятиях. Таким образом, данная статья направлена на изучение этапов, видов, методов менеджмента рисков информационной безопасности, что позволит читателям глубже понять важность этого процесса и применить полученные знания в своей профессиональной деятельности.*

Ключевые слова: *информационная безопасность, кибератака, методы, риски, угрозы.*

Pershikova E.D., Suslova V.S., Volkova D.G.
students of the Faculty of Economics and Management,

Moscow State University of Technology and Management named after K.G. Razumovsky

Academic Supervisor: Shveyova E.I., PhD in Economics

Moscow State University of Technology and Management named after K.G. Razumovsky

Moscow, Russia

INFORMATION SECURITY RISK MANAGEMENT AS A CONTINUOUS PROCESS

Abstract: *This article examines information security risk management as a continuous process that requires integration into the strategic planning of organizations. The key stages of risk management are analyzed: identification, assessment, response and monitoring. Particular attention is paid to vulnerabilities in the digital environment and in industrial enterprises. Thus, this article is aimed at studying the stages, types, methods of information security risk management, which will allow readers to better understand the importance of this process and apply the acquired knowledge in their professional activities.*

Keywords: *information security, cyber attack, methods, risks, threats.*

В наше время компании хранят большинство информации в цифровом формате. Переход от бумажных носителей к цифровым системам значительно упростил процесс хранения и обработки данных, но одновременно повысил риски утечек и кибератак. Под кибератакой следует понимать любую попытку несанкционированного доступа к информационной системе.

В условиях современной цифровой экономики обеспечение информационной безопасности — одна из ключевых задач любой организации. Из-за большого влияния информационных технологий,

которые прочно вошли в нашу жизнь, угрозы кибератак и утечек данных приобретают все большую актуальность. Эффективная защита информации требует комплексного подхода к управлению рисками, который должен рассматриваться не как разовая мера, а как непрерывный процесс.

Менеджмент рисков информационной безопасности включает в себя идентификацию, оценку и управление потенциальными угрозами, которые могут повлиять на конфиденциальность, целостность и доступность данных. Этот процесс охватывает весь жизненный цикл системы управления информацией, начиная от анализа существующих уязвимостей и заканчивая внедрением мер защиты и мониторингом их эффективности.

Тщательно проанализировав материалы по данной теме, можно дать следующее определение информационной безопасности: это защита всех видов информации (как физических документов, так и данных, хранящихся на компьютерах) от несанкционированного доступа, изменения или удаления данных, а также предотвращение утечек данных и других угроз, связанных с хранением и передачей информации. Стоит отметить, что информационную безопасность часто путают с кибербезопасностью, которая фокусируется исключительно на защите цифровых устройств и интернета от атак злоумышленников, включая защиту от различных вирусов, троянов, фишингов и прочее. [11]

Внедрение процессов по защите информации становится не только важнейшим условием для стабильного развития бизнеса, но и законодательным требованием, так как в современных реалиях цифровой экономики необходимость всесторонней кибербезопасности очевидна. Угрозы информационной безопасности присутствуют в любом виде бизнеса. Нередко компании проводят аудит безопасности (независимая проверка системы защиты данных) для оценки рисков и создания

стратегии сопротивления хакерским атакам, чтобы сохранить конфиденциальности информации.

Под риском информационной безопасности понимается потенциальная возможность того, что уязвимость будет использована для создания угрозы активам, что может привести к ущербу для организации. Активы в свою очередь являются ценностью любой компании, они представляют собой блага, которые организация может использовать в своей деятельности. На рисунке 1 перечислены основные виды активов.

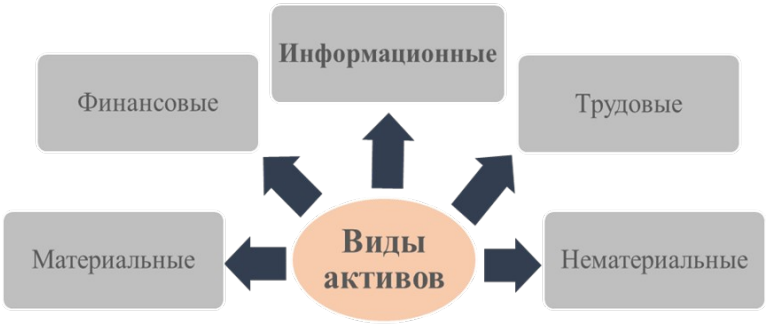

Рисунок 1 - Основные виды активов.

Разберем каждый вид более подробно. Под материальными активами подразумеваются физические объекты, такие как: продукция, услуги, материалы, комплектующие, оборудование, транспорт, здания. Нематериальные активы представляют собой неосязаемые ресурсы, например, компьютерные программы, приложения, товарные знаки, лицензии, патенты, авторские права и др. Трудовые активы — это ресурсы, связанные с работниками организации: их знания, навыки, опыт и трудовые отношения. Финансовые активы — это денежные средства. Например, счет в банке, поступления за продукцию и услуги, расчеты по закупкам, кредиты и займы, налоги, ценные бумаги. И наконец информационные активы — это данные и информация, которыми оперирует организация. В это понятие входят: финансовая информация,

данные о продажах и закупках, базы данных клиентов, стратегические планы, содержание корпоративного сайта и другое. Правильное управление информационными активами помогает защитить компанию от таких рисков, как утечки, кражи и уничтожение важных сведений.

Для расчета величины риска используется формула, в которой под величиной риска условно понимают произведение вероятности негативного события и размера ущерба. Под вероятностью события понимается произведение вероятности реализации угрозы информационной безопасности, а также уязвимостей информационной безопасности, выраженные в качественной или количественной форме. Наглядно данная формула представлена на рисунке 2.

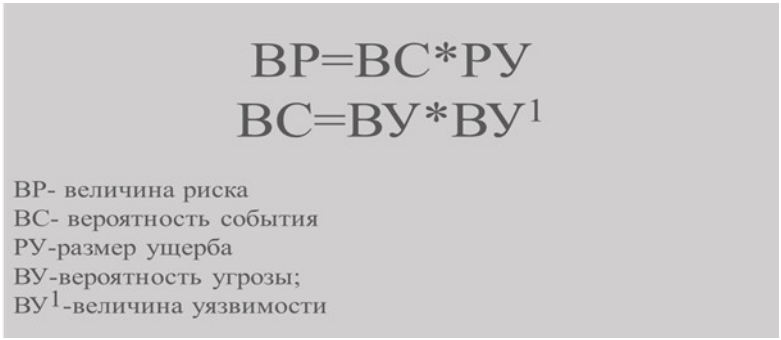

Рисунок 2 - Формула расчета величины риска.

Данная формула для вычисления величины риска позволяет количественно оценить потенциальные угрозы, которые могут воздействовать на информационные ресурсы, включая аспекты конфиденциальности, целостности и доступности данных. [8]

Е. П. Ильин выделяет три основных вида рисков информационной безопасности:

1. Случайные. Риски, связанные с действиями непредвиденных событий; стечение обстоятельств, приводящее к неблагоприятным последствиям. Данные риски не зависят от рискованных решений или действий человека. Среди типичных примеров – чрезвычайные ситуации, перебои электроэнергии, повреждение коммуникационных каналов и др.

2. Субъективные. Возникают из-за ошибок и некорректных действий персонала в процессах хранения и обработки информации. Примеры данных рисков: игнорирование внутренних правил и инструкций безопасности в компании (несанкционированный доступ к сведениям, использование незащищенных каналов информации)

3. Объективные. Возникают в процессе использования систем защиты и сопутствующего технического оборудования. Риски возникают в результате проникновения в информационную систему вирусов, вредоносного программного обеспечения, внедрения оборудования для слежки. Такой вид рисков нельзя исключить полностью, так как злоумышленники постоянно придумывают новые приемы, а системы защиты имеют несовершенства. [1]

На основании всего вышеперечисленного становится очевидно, что любой компании необходимо выявлять информационные риски для защиты своих данных, это помогает предотвратить утечки и как следствие финансовые потери. Выявление рисков информационной безопасности и управление ими включает несколько ключевых этапов.

Первоначально проводится идентификация рисков, то есть выявление потенциальных угроз и уязвимостей, способных нанести ущерб информационным активам организации. Также на данном этапе обнаруживаются внутренние и внешние факторы, которые могут привести к инцидентам безопасности. Параллельно составляется подробный перечень информационных активов организации: от данных до оборудования.

Просто знать об угрозах – недостаточно. Вторым этапом в проведении оценки риска является анализ риска и его комплексная оценка. Эти процедуры позволяют организации оценить потенциальный ущерб и сформировать приоритетные меры защиты. На основании полученных данных формулируются рекомендации для руководства, которое будет

принимать дальнейшие решения. На основе анализа выбираются наиболее эффективные методы управления риском. Для этого формируется команда специалистов, которая анализирует доступные стратегии,такие как избежание, снижение, передача или принятие рисков. Обратимся к более детальному рассмотрению данных стратегий. Под избежанием рисков понимается стратегия, при которой организация изменяет свои планы или процессы, чтобы полностью устранить риск или его источник. [2]

Снижение рисков подразумевает под собой стратегию, направленную на уменьшение вероятности возникновения риска или его последствий через внедрение контрольных мер и процедур.

Принятие рисков включает в себя стратегию, при которой организация осознанно принимает риск, признавая его неизбежность и готовясь к возможным последствиям. Компании необходимо выбрать одну из четырех стратегий управления, которая будет наиболее эффективно реагировать на выявленные риски. От верности этого выбора напрямую зависит способность организации защитить свои информационные ресурсы. После того как риски идентифицированы, проанализированы и выбраны наиболее подходящие методы управления, наступает этап их практической реализации. Практическое применение выбранных методов основывается на внедрении процессов, направленных на защиту информации, которые становятся частью повседневной работы компании. Работа по управлению рисками не заканчивается на внедрении защитных мер, важно оценивать, насколько эти меры помогают достичь заданного уровня безопасности. И именно поэтому важно проводить непрерывный мониторинг факторов риска, а также совершенствовать систему управления рисками по мере необходимости. [3]

Качественный метод	Количественный метод
Субъективный процесс	Более объективный процесс
Сильная зависимость от опыта и знаний исследователя,	Требует больше ресурсов
Чаще всего неприемлем для сложных сценариев, имеющих дело с технической неопределенностью	Рекомендован для сложных сценариев и критически важных систем безопасности
объекту оценки присваивается показатель, систематизированный по трехбалльной (низкий, средний, высокий), пятибалльной или десятибалльной шкале.	Результат может выражаться в процентах, деньгах, времени и др.
Используемые методики: опросы целевых групп, интервьюирование, анкетирование или личные встречи.	Используемые методики: формулы, расчеты, анализ чувствительности, метод сценариев и др.

Рисунок 3 - Сравнение качественного и количественного метода для анализа рисков информационной безопасности.

На рисунке 3 приведено сравнение количественного и качественного методов. Существуют различные методики для анализа рисков информационной безопасности. Нельзя точно сказать, какой метод предпочтительнее, так как у каждого из методов есть свои преимущества и недостатки, и угрозу необходимо анализировать со всех сторон. Однако стоит отметить, что качественный анализ рисков предшествует количественному. [5]

Но если нарушители все же смогли успешно преодолеть выстроенные защитные меры и достичь своих целей, то говорят, что произошла кибератака. Иными словами, кибератака — это целенаправленное вредоносное воздействие на актив для нарушения его работы или для реализации киберугрозы (т.е. нарушение целостности, конфиденциальности, доступности информации). Также часто это называют взломом. Взлом — это незаконное получение доступа к конфиденциальной информации компании. Ущерб от реализации кибератаки может быть прямым или непрямым.

Прямой ущерб — это очевидные, явные и просто прогнозируемые потери компании. Например, разглашение тайны производства, разрушение активов или снижение их стоимости. Непрямой ущерб — это качественные или косвенные потери. Качественные потери представляют

из себя снижение эффективности организации, потерю клиентуры, падение качества производимых товаров или предоставляемых услуг. Под косвенными потерями мы понимаем потерю репутации, снижение прибыли, непредвиденные расходы и т.д.

Своевременное выявление рисков информационной безопасности крайне важно для эффективной работы промышленных предприятий. Такие предприятия, взаимодействующие с автоматизированными системами управления технологическими процессами (АСУТП), особенно подвержены рискам, связанным с незаконным получением доступа к секретным информационным ресурсам, безопасностью конфиденциальных данных, сбоями на серверах и пр.

Изучив несколько реальных примеров, с которыми столкнулись промышленные предприятия по всему миру, было выявлено, с какими последствиями может столкнуться компания, если она недостаточно обеспечивает свою информационную безопасность. Так, например, кибератака может привести к следующему:

1. Остановка производства. Во время одной из кибератак на сервера Honda, компании по производству автомобилей пришлось остановить рабочий процесс на нескольких заводах из-за того, что информационная система компании была зашифрована злоумышленниками. На восстановление работоспособности и обеспечение дальнейшего нормального функционирования бизнес-процессов было потрачено немало ресурсов. Компания потерпела финансовые убытки.

2. Нарушение технологических процессов. Работа крупнейшей в Соединенных штатах Америки компании по поставке топлива — Colonial Pipeline — была нарушена из-за атаки вируса на компьютерные системы компании. Неделя атаки обернулась серьезными потерями: закрылась половина заправочных станций в нескольких штатах, выросли оптовые цены на бензин, возник ажиотажный спрос на топливо.

3. Нарушение бизнес-процессов. В феврале 2020 года в результате хакерской атаки на INA — нефтяную компанию из Хорватии — произошел сбой, фирма не могла выставлять счета-фактуры, фиксировать использование карт лояльности, выпускать новые мобильные ваучеры и принимать от клиентов плату за топливо. Причиной нарушения бизнес-процессов стала программа-вымогатель Clop, зашифровавшая данные на внутренних серверах компании.

На основании изучения данных случаев можно сделать вывод, что главная задача специалистов по информационной безопасности — оценка вероятности наступления рисков информационной безопасности, а также последствий наступления кибератак, и построение на основе этой оценки эффективной системы защиты данных.

Любая уязвимость может привести к большим финансовым потерям. Однако не все компании знают, что уязвимости могут скрываться в самых обычных, на первый взгляд, проблемах, с которыми сталкиваются большинство: низкая защищенность сети; недостаточная конфигурация устройств; отсутствие фильтрации трафика; использование словарных паролей; использование устаревшего программного обеспечения.

По результатам проектов по анализу защищенности было установлено, что в 91% промышленных организаций внешний злоумышленник может проникнуть в корпоративную сеть. [9] Оказавшись во внутренней сети, он может получить учетные данные пользователей и полный контроль над инфраструктурой или украсть конфиденциальные данные: информацию о партнерах и сотрудниках компании, почтовую переписку и внутреннюю документацию. Подробная статистика представлена на рисунке 3.

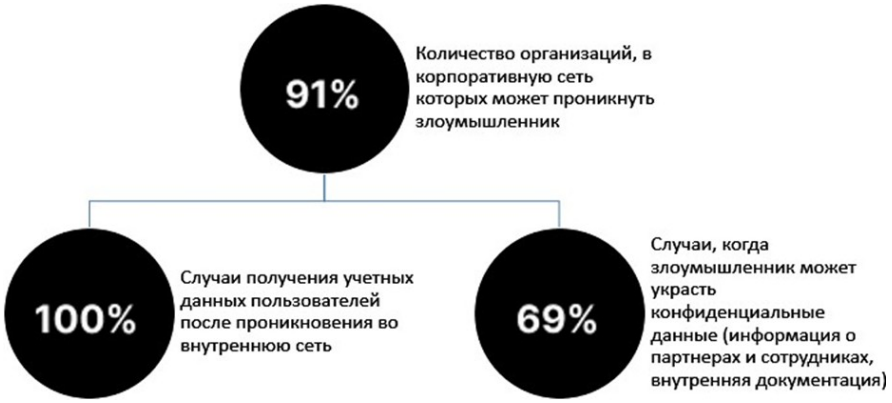

Рисунок 4 - Статистика случаев проникновения злоумышленников в корпоративную сеть и последствий взлома.

Проанализировав информацию на рисунке 4, был сделан вывод о том, что процесс изучения, анализа и оценки рисков информационной безопасности должен быть непрерывным на протяжении всей жизни предприятия, так как уровень защищенности большинства промышленных предприятий близок к нулю.

Использованные источники:

1. Болдыревский П. Б. Анализ и оценка рисков информационной безопасности бизнес-процессов // Вестник Нижегородского университета им. Н. И. Лобачевского. Серия: Социальные науки. — 2023. — № 4 (72). — С.18-24.

2. Легчекова Е. В., Титов О. В. Метод расчета рисков информационной безопасности// Сборник научных статей международной научно–практической конференции «Проблемы и перспективы электронного бизнеса». - Гомель: Белорусский торгово–экономический университет потребительской кооперации, 2017. - С. 87-89.

3. Зайнутдинова Е. В. Конфиденциальность персональных данных в ситуации киберугроз // Юридическая наука и практика. - 2023. - № 19 (3). - С. 38-46.

4. Карунная Я.А. Проблемы защиты персональных данных в условиях цифровой трансформации // Юридическая наука и практика. - 2023. - № 19 (3). - С. 47-56.

5. Риски ИБ в промышленных компаниях / PT Security [Электронный ресурс] // PostiveTechnologies : [сайт]. - URL: https://www.ptsecurity.com/ru-ru/research/analytics/ics-risks-2021/ (дата обращения: 17.12.2024).

6. Управление рисками проекта / НОУ ИНТУИТ [Электронный ресурс] //Intuit:[сайт]-URL:https://intuit.ru/studies/professional_retraining/964/courses/267/lecture/6 806?page=6&ysclid=m4spcn30c928952571 (дата обращения: 18.12.2024).

7. Difference Between Cyber Security and Information Security / [Электронный ресурс] // GeeksforGeeks: [сайт]. — URL: https://www.geeksforgeeks.org/difference-between-cyber-security-and-information-security/ (дата обращения: 16.12.2024).