*Завоеванов Александр Сергеевич, студент магистратуры*

*(Южно-Уральский государственный гуманитарно-педагогический университет, г. Челябинск, Россия)*

*Куприянов Кирилл Александрович, студент магистратуры*

*(Южно-Уральский государственный гуманитарно-педагогический университет, г. Челябинск, Россия)*

##### *Научный руководитель д.т.н Дмитриев Михаил Сергеевич*

*(Южно-Уральский государственный гуманитарно-педагогический университет, г. Челябинск, Россия)*

**РОЛЬ ОТДЕЛА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СТРУКТУРЕ СЛУЖБЫ БЕЗОПАСНОСТИ**

*Данная научная статья представляет исследование роли отдела информационной безопасности в структуре службы безопасности.*

*В статье проанализированы функции отдела, его влияние на общую безопасность организации. Исследование основано на анализе текущих исследований, статистических данных и мнениях экспертов в области защиты персональных данных.*

*Ключевые слова: защита информации, отдел информационной безопасности, ключевые функции, проблема взаимодействия, проблема непонимания.*

*THE ROLE OF THE INFORMATION SECURITY DEPARTMENT IN THE STRUCTURE OF THE SECURITY SERVICE*

*This scientific article presents a study of the role of the information security department in the structure of the security service. The article analyzes the functions of the department, its impact on the overall security of the organization. The study is based on an analysis of current research, statistical data and opinions of experts in the field of personal data protection.*

*Keywords: information protection, information security department, key functions, interaction problem, misunderstanding problem.*

*Zavoevanov Alexander Sergeyevich, master student*

*(South Ural State Humanitarian Pedagogical University, Chelyabinsk, Russia)*

*Kupriyanov Kirill Alexandrovich, master student (South Ural State Humanitarian Pedagogical University, Chelyabinsk, Russia)*

В современном мире, где информационные технологии проникают во все сферы жизни, роль отдела информационной безопасности становится критически важной для обеспечения защиты данных и предотвращения угроз. С увеличением числа кибератак и утечек информации, организации сталкиваются с необходимостью создания эффективных структур, способных противостоять этим вызовам. Проблема заключается в том, что компании не уделяют должного внимания интеграции информационной безопасности в общую систему безопасности, что может привести к серьезным последствиям.[1] На текущий момент, как это ни прискорбно, информационная безопасность для нашей страны — это чаще всего модная вещь, с не совсем понятным назначением. Исходя из этого непонимания складывается и все проблемы информационной безопасности в организациях и, собственно, организации самой информационной безопасности.[2]

Цель данной работы заключается в анализе функций и задач отдела информационной безопасности, а также в целесообразности его интеграции с другими подразделениями службы безопасности. Важно понять, как отдел информационной безопасности может эффективно координировать свои действия с IT-отделом и подразделениями физической и кадровой безопасности для создания комплексной системы защиты.

Ключевыми персонами, влияющими на эту тему, являются руководитель служб безопасности, специалист по информационной безопасности и юрист в сфере защиты персональных данных, IT-эксперт. Их взаимодействие и понимание общих целей могут существенно повысить уровень защиты информации в организации. Кроме того, современные угрозы, такие как кибератаки, фишинг и внутренние угрозы, требуют от отдела информационной безопасности постоянного анализа и адаптации к новым условиям. [3]

Актуальность темы для России и мира обусловлена растущими рисками в области кибербезопасности и необходимостью защиты ключевой системы информационной структуры. Террористические и криминальные структуры интенсивно совершенствуют методы и способы использования информационных технологий и средств уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним официальных пользователей, а также дезорганизации работы технических средств, вывода из строя телекоммуникационных сетей, компьютерных систем, всего высокотехнологичного жизнеобеспечения обществ Такое применение информационных технологий придает имсвойства так называемого информационного оружия. Для нанесения значительного ущерба интересам государства и общества информационное оружие может быть применено и в мирное время, особенно террористическими организациями. В рамках данной темы можно рассмотреть задачи, такие как оценка текущих угроз, разработка стратегий защиты информации, а также внедрение современных технологий для повышения эффективности работы отдела. [4]

Таким образом, данное исследование направлено на глубокий анализ роли отдела информационной безопасности в структуре службы безопасности, что позволит выявить ключевые аспекты его функционирования и предложить рекомендации по улучшению работы в условиях современных вызовов. [5]

Отдел информационной безопасности может быть как структурным подразделением службы безопасности, так и самой компании. Основными задачами этого отдела являются:

Базис работы отдела информационной безопасности сводится к трем векторам: планирование и подготовка к действиям в экстренных ситуациях, ежедневные действия отдела, проверка выполнения задач и работоспособности средств защиты. [6]

Основной целью работы отдела представляет собой гарантирование безопасности функционирования компании.   
Анализ деятельности компаний показал трудности в координации работы подразделений, вызванные внутренними противоречиями. [7]

Однако, опыт подтверждает, что эффективно сформированный отдел информационной безопасности способен правильно решить несколько организационных проблем:

• Правильно найти свое место в структуре компании;

•Организовать взаимодействие подразделений внутри службыбезопасности, добиться эффекта синергии;

•На практике доказать свою состоятельность;

•Правильно выстроить отношения в компании по вертикали;

•Правильно выстроить отношения в компании по горизонтали;

•Построить эффективные контакты во внешней среде.

Небольшие организации в основном ограничиваются группами внутренней безопасности, состоящими из охранников и персонала, занимающегося настройкой и ремонтом технических средств защиты. [8] Однако крупным организациям и корпорациям необходимо внимательно и серьезно подходить к защите конфиденциальной информации и организовывать такую службу безопасности, которая позволит своевременно обнаружить и максимально ослабить воздействие различного рода опасностей и угроз в условиях конкуренции и хозяйственного риска.

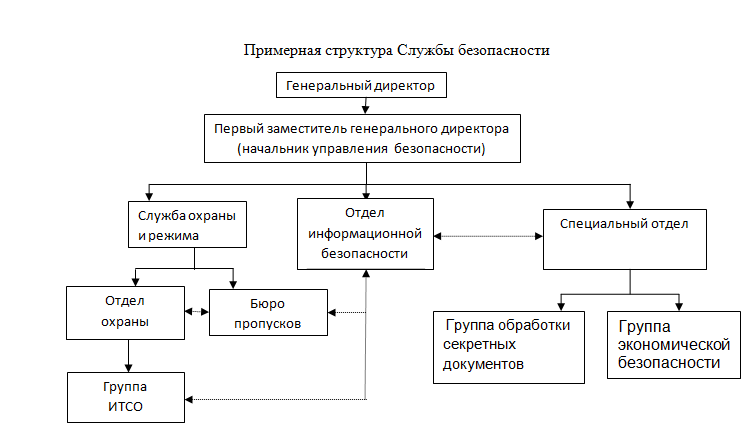


Рисунок 1. Примерная структура Службы безопасности

Полномочия у службы безопасности, как правило, очень высокие, поэтому распоряжения отдела информационной безопасности будут вынуждены выполнять все другие структурные подразделения предприятия.   
В таком случае главное препятствие — конфликт интересов. Работа ИБ, в частности, это контроль за выполнением ит-специалистами правил, предписаний и регламентов. При проведении аудита, опять же, в случае невыполнения каких-то пунктов отделом ИТ может быть не подписан протокол руководителем и так далее. И опять же вопрос с различием направлений, так как информационная безопасность имеет лишь опосредованное отношение к ИТ. Большая часть с ИТ не совсем стыкуется.  
Из положительных моментов — горазд проще внедрение каких-то систем, фактически исполнители у вас под рукой.  
В любом из этих архетипов есть проблема пассивного сопротивления из-за количества уровней согласования. [9]

Идеальной вертикалью подчинения будет непосредственно генеральному или первому заместителю генерального директора. Отличным вариантом был бы заместитель по информационной безопасности, но такой вариант в России не практикуется. Такой расклад позволил бы получить плюсы первого варианта, при сокращении вертикали согласования и времени принятия решения. [10]

Существенной проблемой является непонимание в полной мере руководством сути работы и её цели, а также задачи и как следствие-непонимание предлагаемых решений.  
Отсюда проблема финансирования по остаточному принципу, торможение проектов и каких-то внедрений и другие неприятные факторы.  
Подобное отношение отчасти оправдано, в виду того, что ит-специалисты и специалисты безопасности не умеют коммуницировать с бизнесменами. Конструктивному общению мешает предвзятость подтверждения. Бизнес говорить на языке бухгалтерского учета, финансов экономики, не забывая при этом про маркетинг, управление персоналом, операции и т.д., Основные принципы и терминология, лежащие в основе бухгалтерского учета, финансов и экономики, определяют решения в компаниях.  внедрение той или иной системы безопасности напрямую прибыль не приносит и нужно считать выгоду от нереализованных потерь.  
2-мя или более альтернативами:

* как было раньше и с какими затратами мы будем сталкиваться каждый раз при повторении
* сколько нам нужно потратить, что бы этого не повторялось (в кооперации с первым пунктом — через какое время мы вернём стоимость решения в отношении к потерям от нереализованных потерь)
* еще один вариант решения, промежуточный, но с не менее точным расчётом. [11]

Управление отделом информационной безопасности, это не то же, что и управление системой информационной безопасности, пусть даже тут работа и связана с людьми на 90%. Для результативного руководства отделом информационной безопасности необходимо уметь объяснять руководству не только преимущества от защиты информации, но и потери от её отсутствия.

**Список литературы**

1. Романова С. создание и организационная структура служб безопасности предприятий [Текст] / Романова С. // "Экономика и социум" . — 2021. — № №5 (84) ч.2. — С. 262-266.

2. BeaVisS Немного об организации отдела информационной безопасности / BeaVisS [Электронный ресурс] // Хабр : [сайт]. — URL: https://habr.com/ru/articles/233357/ (дата обращения: 03.01.2025).

3. Как считать эффективность ИБ-отдела. Три рабочих варианта // IT ChannelNews URL: https://www.novostiitkanala.ru/news/detail.php?ID=168828 (дата обращения: 26.01.2025).

4. Главное управление информационных технологий [Электронный ресурс] // customs.gov.ru - Режим доступа: https://customs.gov.ru/folder/86278, свободный. - Загл. с экрана [Открыть](https://customs.gov.ru/folder/86278)

5. Отдел защиты интеллектуальной собственности - Управление ... [Электронный ресурс] // www.mirea.ru - Режим доступа: https://www.mirea.ru/about/the-structure-of-the-university/scientific-structural-unit/research-division/the-department-of-innovative/, (дата обращения: 26.01.2025).

6. Положение о Совете Безопасности Российской Федерации [Электронный ресурс] // www.scrf.gov.ru - Режим доступа: http://www.scrf.gov.ru/about/regulations/, (дата обращения: 26.01.2025).

5. Общая информация - Управление информатизации - РТУ МИРЭА [Электронный ресурс] // www.mirea.ru - Режим доступа: https://www.mirea.ru/about/the-structure-of-the-university/administrative-structural-unit/informatization/obshchaya-informatsiya/, (дата обращения: 26.01.2025).

7. Место и роль персонала в информационной безопасности ... [Электронный ресурс] // cyberleninka.ru - Режим доступа: https://cyberleninka.ru/article/n/mesto-i-rol-personala-v-informatsionnoy-bezopasnosti-organizatsii, (дата обращения: 26.01.2025).

8. УМО ИБ - Учебно-методическое объединение высших учебных ... [Электронный ресурс] // www.isedu.ru - Режим доступа: http://www.isedu.ru/, свободный. - (дата обращения: 26.01.2025).

9. Роль образовательной организации в обеспечении ... [Электронный ресурс] // cyberleninka.ru - Режим доступа: https://cyberleninka.ru/article/n/rol-obrazovatelnoy-organizatsii-v-obespechenii-informatsionnoy-bezopasnosti-uchaschihsya, (дата обращения: 26.01.2025).

10. Подробная информация :: Федеральная Служба Безопасности ... [Электронный ресурс] // www.fsb.ru - Режим доступа: http://www.fsb.ru/fsb/npd/more.htm%21id%3D10340801%40fsbNpa.html, (дата обращения: 26.01.2025).

11. Кафедра: Информационная безопасность (ИБ) [Электронный ресурс] // mtuci.ru - Режим доступа: https://mtuci.ru/about\_the\_university/structure/769/, (дата обращения: 26.01.2025).