УДК 351.83

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРОЦЕССЕ ДИСТАНЦИОННОГО ОБУЧЕНИЯ НА ОСНОВЕ КАДРОВЫХ РЕСУРСОВ

Гудков Владимир Владимирович
магистрант кафедры Государственное и муниципальное управление,
Брянский филиал РАНХиГС (г Брянск, Россия)
gudvova32@mail.ru

Филичева Татьяна Алексеевна
доцент кафедры Брянского филиала РАНХиГС,
кандидат технических наук, доцент (г. Брянск, Россия)
fta@br.ranepa.ru

Ключевые слова: *информационная безопасность, дистанционное обучение, кадровые ресурсы, компетентность кадров отдела безопасности.*

Keywords: *information security, distance learning, human resources, competence of the personnel of the security department.*

Аннотация. *В данной статье приведены факторы опасности, влияющие на информационную безопасность в процессе дистанционного обеспечения. Разработаны критерии компетентности кадровых ресурсов отдела безопасности компании.*

Электронный архив библиотеки имени А. Кулешова

Annotation. *This article presents the hazards that affect information security in the process of remote provision. Criteria for the competence of human resources of the security department of the company have been developed.*

В настоящее время множество организаций повышают знания и квалификацию своих сотрудников с помощью дистанционного обучения. Дистанционное обучение имеет свои преимущества перед привычным очным: каждый сотрудник выбирает свой темп обучения, последовательность уроков, а информация предоставляется в легко усваиваемом формате.

Однако дистанционное обучение несет свои риски, в первую очередь это потеря и хищение личных данных сотрудников. Информационная безопасность в данном случае зависит не только от применяемого технического оснащения и защиты, но и от компетентности сотрудников, обеспечивающих защиту личных данных в сервисе. Поэтому актуальным является рассмотрение необходимых навыков сотрудников службы безопасности в компании.

На информационную защиту в организации при дистанционном обучении влияет кадровая безопасность. Кадровая безопасность – это процесс защиты информационной безопасности от неблагоприятных воздействий, связанных с работниками компании, их интеллектуальным потенциалом и трудовыми отношениями в целом.

Целями обеспечения кадровой безопасности являются [2]:

– предотвращение угроз безопасности: хищения, разглашения, утраты, утечки, искажения и уничтожения служебной информации;

– обеспечение стабильного дистанционного обучения;

– защита данных сотрудников, их жизни и здоровья.

Угрозы, связанные с сотрудниками службы безопасности, которые имеют влияние на информационную безопасность, могут быть внутренними и внешними.

Внутренние угрозы – это неумышленные или умышленные действия персонала, приводящие к ущербу. Например, недостаточная квалификация сотрудников, отсутствие мотивации сотрудников, уход квалифицированных сотрудников, некачественные проверки кандидатов при приеме на работу.

Внешние угрозы – это явления, которые не зависят от действий персонала. Например, давление на сотрудников извне, попадание сотрудников в различные виды внешней зависимости, хедхантинг.

Электронный архив библиотеки МГУ имени А.А. Кулешова

Полностью избежать данных рисков невозможно, но снизить вероятность их возникновения можно с помощью управления кадровыми ресурсами отдела безопасности. Для этого необходимо определить, какими компетенциями должен обладать сотрудник отдела безопасности, чтобы обеспечить надлежащий контроль за информационными потоками при дистанционном обеспечении.

Для составления списка компетенций была использована Модель компетентности Министерства труда США (DOL), которая состоит из набора блоков, разбитых на уровни, содержащих конкретные наборы связанных компетенций [3]. В рамках этой структуры уровни сгруппированы в три блока: базовые компетенции, отраслевые и профессиональные [1].

В соответствии с этими уровнями для сотрудника, отвечающего за информационную безопасность при дистанционном обучении, были составлены следующие компетенции:

1) базовый уровень: общие (ясное и логичное выражение мыслей, твердость и нравственность личности, способность к приспособлению к существующим требованиям); академические (наличие логики и критического мышления, умение быстро находить решение, навыки использования ПК, Интернета, MS Office); компетенции в области информационной безопасности (эффективная работа в группе и по одиночке, прогнозирование долгосрочных потребностей, принятие решений на фактах);

2) отраслевой уровень: общепромышленные технические компетенции (знания в области оценки и работы с рисками в кризисных ситуациях, расследование компьютерных инцидентов, обеспечение защиты данных от хищений и изменений); отраслевые (использование и эффективное применение технических средств защиты информации, выявление и анализ рисков информационной безопасности, выявление неблагоприятных ситуаций, проведение мер по обеспечению целостности и конфиденциальности информации);

3) профессиональный уровень: профессиональные (лидерство, эффективность, стратегическое мышление, непрерывное обучение, постоянное подтверждение соответствия занимаемой должности).

Данный список компетенций может служить базой для найма и аттестации сотрудников службы безопасности, что поможет организации проводить отбор квалифицированных специалистов в области информационной безопасности. Соискатели, ориентирующиеся на данные компетенции, будут более востребованными на рынке труда. Данный

Электронный архив библиотеки МГУ имени А.А. Кулешова

перечень компетенций поможет сотрудникам и руководству обеспечивать надлежащий уровень информационной безопасности при осуществлении дистанционного обучения специалистов.

Список литературы

1. Васильева, Д. С. Модель компетентности специалиста по информационной безопасности в современных условиях / Д. С. Васильева, А. В. Шабурова // Интерэкспо Гео-Сибирь. – 2020. – № 1. – С. 53–59.
2. Климов, Д. В. Кадровая безопасность: понятие, внутренние и внешние угрозы, группы риска // Вестник Прикамского социального института. – 2019. – № 2(83). – С. 41–44.
3. Хуторский, А. В. Компетенции в образовании: опыт проектирования: сб. науч. тр. – М.: Научно-внедренческое предприятие «ИНЭК», 2007. – 327 с.